



PCT

特許協力条約に基づいて公開された国際出願

<p>(51) 国際特許分類6 G11B 20/10</p>	<p>A1</p>	<p>(11) 国際公開番号 WO00/05716</p> <p>(43) 国際公開日 2000年2月3日(03.02.00)</p>
<p>(21) 国際出願番号 PCT/JP99/03887</p> <p>(22) 国際出願日 1999年7月21日(21.07.99)</p> <p>(30) 優先権データ 特願平10/206967 1998年7月22日(22.07.98) JP 特願平10/289831 1998年10月12日(12.10.98) JP</p> <p>(71) 出願人 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP] 〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)</p> <p>(72) 発明者 田川健二(TAGAWA, Kenji) 〒576-0021 大阪府交野市妙見坂5丁目5番地305号 Osaka, (JP) 南 賢尚(MINAMI, Masataka) 〒656-2311 兵庫県津名郡東浦町久留麻2349-1 Hyogo, (JP) 小塚雅之(KOZUKA, Masayuki) 〒572-0024 大阪府寝屋川市石津南町19番1-1207号 Osaka, (JP)</p>		<p>(74) 代理人 中島司朗(NAKAJIMA, Shiro) 〒531-0072 大阪府大阪市北区豊崎三丁目2番1号 淀川5番館6F Osaka, (JP)</p> <p>(81) 指定国 AU, CN, ID, KR, MX, SG, 欧州特許 (DE, FR, GB, IT, NL)</p> <p>添付公開書類 国際調査報告書</p>
<p>(54)Title: DIGITAL DATA RECORDING DEVICE AND METHOD FOR PROTECTING COPYRIGHT AND EASILY REPRODUCING ENCRYPTED DIGITAL DATA AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM</p> <p>(54)発明の名称 著作権を保護し、記録媒体に記録された暗号化されたデジタルデータの再生を容易にするデジタルデータ記録装置及びその方法並びにそのプログラムを記録したコンピュータ読み取り可能な記録媒体</p> <p>(57) Abstract A data transmitting/receiving unit receives electronically allotted encrypted digital data for recording on a primary recording medium. Digital data use provider-dependent different encryption systems and contain attribute information describing encryption systems. Digital data retrieved at a data retrieving unit is judge for an encryption system at a judging unit and is decoded at one proper decoding unit. An inherent information acquiring unit acquires identification information of a secondary recording medium or a reproducing device depending on whether or not the second recording medium is mountable/demountable to/from the reproducing device. An encryption system instructing unit selects one encrypting unit out of a plurality of encrypting units based on the acquired identification information. The one encrypting unit creates an encryption key based on the identification information and encrypts digital data. A recording unit records digital data on the secondary recording medium, and an accounting unit charges costs according to accounting information described in the attribute information.</p> <div data-bbox="1023 1323 1461 1575"> </div> <div data-bbox="1104 1575 1331 1953"> <p>A デジタルデータ記録装置</p> <p>A ... DIGITAL DATA RECORDING DEVICE</p> <p>100 ... DATA TRANSMITTING/RECEIVING UNIT</p> <p>101 ... RECEIVING UNIT</p> <p>102 ... PRIMARY RECORDING MEDIUM</p> <p>103 ... DATA RETRIEVING UNIT</p> <p>104 ... JUDGING UNIT</p> <p>105 ... DECODING UNIT GROUP</p> <p>106 ... FIRST DECODING UNIT</p> <p>107 ... SECOND DECODING UNIT</p> <p>108 ... KEY DECODING UNIT</p> <p>109 ... ENCRYPTION SYSTEM INSTRUCTING UNIT</p> <p>110 ... ENCRYPTING UNIT GROUP</p> <p>111 ... FIRST ENCRYPTING UNIT</p> <p>112 ... SECOND ENCRYPTING UNIT</p> <p>113 ... KEY ENCRYPTING UNIT</p> <p>114 ... SECONDARY RECORDING MEDIUM</p> <p>115 ... RECORDING UNIT</p> <p>116 ... INHERENT INFORMATION ACQUIRING UNIT</p> <p>117 ... INSTRUCTION RECEIVING UNIT</p> <p>118 ... ACCOUNTING UNIT</p> </div>		

(57)要約

データ送受信部は、電子配信される暗号化されたデジタルデータを受信し、一次記録媒体に記録する。デジタルデータは、提供者ごとに暗号方式が異なり、暗号形式を記載した属性情報を含んでいる。データ取出部で取り出されたデジタルデータは、判定部で暗号形式が判定され、適切な一の復号化部で復号される。固有情報取得部は、二次記録媒体が再生装置に対して着脱可能か否かで二次記録媒体又は再生装置の識別情報を取得する。暗号方式指示部は、取得された識別情報に従い、複数の暗号化部から一の暗号化部を選ぶ。一の暗号化部は、識別情報を基に暗号鍵を生成し、デジタルデータを暗号化する。記録部は二次記録媒体にデジタルデータを記録し、課金部は、属性情報に記載された課金情報に従い課金する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AL	アルバニア	EE	エストニア	LC	セントルシア	SD	スーダン
AM	アルメニア	ES	スペイン	LI	リヒテンシュタイン	SE	スウェーデン
AT	オーストリア	FI	フィンランド	LK	スリ・ランカ	SG	シンガポール
AU	オーストラリア	FR	フランス	LR	リベリア	SI	スロヴェニア
AZ	アゼルバイジャン	GB	ガボン	LS	レソト	SK	スロヴァキア
BA	ボスニア・ヘルツェゴビナ	GD	グレナダ	LT	リトアニア	SL	シエラ・レオネ
BB	バルバドス	GE	グルジア	LU	ルクセンブルグ	SN	セネガル
BF	ブルキナ・ファソ	GH	ガーナ	LV	ラトヴィア	SZ	スワジランド
BG	ブルガリア	GM	ガンビア	MA	モロッコ	TD	チャード
BJ	ベナン	GN	ギニア	MC	モナコ	TG	トーゴ
BR	ブラジル	GW	ギニア・ビサウ	MD	モルドヴァ	TJ	タジキスタン
BY	ベラルーシ	GR	ギリシャ	MG	マダガスカル	TZ	タンザニア
CA	カナダ	HR	クロアチア	MK	マケドニア旧ユーゴスラヴィア	TM	トルクメニスタン
CC	中央アフリカ	HU	ハンガリー		共和国	TR	トルコ
CG	コンゴ	ID	インドネシア	ML	マリ	TT	トリニダード・トバゴ
CH	スイス	IE	アイルランド	MN	モンゴル	UA	ウクライナ
CI	コートジボアール	IL	イスラエル	MR	モーリタニア	UG	ウガンダ
CM	カメルーン	IN	インド	MW	マラウイ	US	米国
CN	中国	IS	アイスランド	MX	メキシコ	UZ	ウズベキスタン
CR	コスタ・リカ	IT	イタリア	NE	ニジェール	VN	ヴェトナム
CU	キューバ	JP	日本	NL	オランダ	YU	ユーゴスラビア
CY	キプロス	KE	ケニア	NO	ノルウェー	ZA	南アフリカ共和国
CZ	チェッコ	KG	キルギスタン	NZ	ニュージーランド	ZW	ジンバブエ
DE	ドイツ	KP	北朝鮮	PL	ポーランド		
DK	デンマーク	KR	韓国	PT	ポルトガル		
				RO	ルーマニア		

明 細 書

著作権を保護し、記録媒体に記録された暗号化されたデジタルデータの再生を容易にするデジタルデータ記録装置及びその方法並びにそのプログラムを記

5 録したコンピュータ読み取り可能な記録媒体

技術分野

本発明は、デジタルデータの著作権保護を図るデジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体に関する。

10

背景技術

近年のインターネットの普及により、P C（パーソナルコンピュータ）を用いて、ホームページ上から好みの音楽データなどをダウンロードにより入手し、クレジットカードなどの決済手段を通じて支払いを行う、いわゆる EC(Electronic

15 Commerce：電子商取引)による音楽流通が広がりつつある。このようなインターネットを通じた EC による音楽流通（以下「電子音楽配信」という。）が普及することは、ユーザがレコード店に行く必要がなくなることを意味し、現在の C D(Compact Disc)中心の音楽流通を大きく変えるものになる可能性を持っている。

20 ところで、音楽を鑑賞するスタイルという点に注目すると、自宅で鑑賞する以外にも、携帯型の再生装置を用いて、通勤、通学途中に鑑賞する、あるいは車の中で鑑賞するというスタイルもかなりの割合を占める。この場合には、音楽データをMD(Mini Disc)等の可搬型の媒体に記録する必要がある。

また、電子音楽配信においては、各社それぞれ独自の暗号方式を採用し、著作権保護を図っている。すなわち、製作会社、流通経路、利用形態等に応じて、それ

25 ぞれ異なる暗号方式を採用している。このため、電子音楽配信によって音楽デ

ータをMD等に記録する場合、流通段階での音楽データをそのまま記録したとき、MD等を再生する再生装置は、各暗号方式に対応して復号化できる装置が求められる。この結果、装置規模が大きくなり、価格の上昇を招き、ユーザにとっては不利益となる。

- 5 一方、ユーザの利益だけを考えるなら、電子音楽配信された音楽データの暗号を復号化してMD等に記録するようにすれば、再生装置は、暗号解読を必要としないので安価なものを提供できることになる。

しかしながら、この場合には、不正なコピーを助長して著作権保護を図ることができない。

10

発明の開示

本発明は、上記課題に鑑みなされたものであり、著作権保護を図り、かつ記録媒体に記録された音楽データを安価なデジタルデータ再生装置で再生することができるデジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体を提供することを目的とする。

15

上記目的は、デジタルデータを記録媒体に記録するデジタルデータ記録装置において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化デジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なる
20 セキュリティレベルを有する暗号化方式の一つでデジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたデジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたデジタルデータを再暗号化させることで達成できる。

- 25 このような構成によって、再生装置で容易に再生できる暗号化部で再暗号化されたデジタルデータを記録媒体に記録することができ、かつ暗号化されている

ので著作権の保護を図ることができる。

ここで、前記記録媒体に記録されたデジタルデータは、再生装置により再生され、前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第1暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第2暗号化部とを有し、前記制御手段は、前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第1暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第2暗号化部によりデジタルデータの暗号化を行わせることができる。

10 このような構成によって、記録媒体がいずれかの再生装置で再生されるときには、その記録媒体の識別情報を基に生成される暗号鍵でデジタルデータを暗号化し、特定の一の再生装置で再生されるときには、その一の再生装置の識別情報を基に生成される暗号鍵でデジタルデータを暗号化することによって、記録媒体に記録されたデジタルデータを再生装置で再生することができる。

15 ここで、前記デジタルデータ記録装置は、更に、前記デジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することができる。

20 このような構成によって、異なるセキュリティレベルを有する暗号化方式の暗号化部を選択することができ、かつ、暗号化部に応じた料金を支払うことができる。

ここで、前記制御手段は、前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化デジタルデータを、前記復号化手段により復号化することを禁止することができる。

25 このような構成によって、暗号化部で暗号鍵を生成できないときには、デジタルデータを復号する処理をなくすことができる。

ここで、前記暗号化手段の有する複数の暗号化部による暗号化されたデジタルデータは、前記通信手段により受信されたデジタルデータの暗号化に比べいずれもセキュリティレベルが低いとすることができる。

このような構成によって、再生装置は、デジタルデータの再生が容易となり、

5 再生装置のコストダウンにつながる。

ここで、前記通信手段により受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたデジタルデータをそれぞれ復号化し、

10 前記制御手段は、前記通信手段により受信された暗号化デジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化デジタルデータを復号化するように前記復号化手段を制御することができる。

15 このよな構成によって、受信されたデジタルデータごとに異なるセキュリティレベルを有する暗号化方式で暗号化されていても、暗号化方式に対応した復号化部を選んで、復号化することができる。

ここで、前記デジタルデータ記録装置は、更に、前記デジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、受信した暗号化デ

20 イジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することができる。

このような構成によって、デジタルデータの復号化と再暗号化とに対応した利用料金が徴収され、著作権の保護を図ることができる。

25 また、上記目的は、デジタルデータを記録媒体に記録するデジタルデータ記録方法において、暗号化されたデジタルデータをデジタルネットワークを

- 介して受信する通信ステップと、前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデジタルデータを前記記録媒体に記録する記録ステップとを有することが達成できる。

このような構成によって、再生装置で容易に再生できる暗号化方式で暗号化されたデジタルデータを記録媒体に記録することができ、かつ、暗号化されているので著作権の保護を図ることができる。

- ここで、前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することができる。

- 15 このような構成によって、通信手段で受信された暗号化されたデジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても、復号化することができる。

- また、上記目的は、デジタルデータを第1記録媒体に記録するデジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデジタルデータを前記第1記録媒体に記録する記録
- 20 ステップとの各ステップをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体で達成できる。

このような構成によって、容易に再生できる暗号化方式で暗号化されたデジタルデータを記録媒体に記録し、かつ、著作権の保護を図る機能のないデジタルデータ記録装置に適用して、このような機能を発揮させることができる。

- ここで、前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求の範囲第 11 項に記載のコンピュータ読み取り可能な記録媒体とすることができる。

このような構成によって、通信手段で受信された暗号化されたデジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても復号化することができる。

15 図面の簡単な説明

図 1 は、本発明に係るデジタルデータ記録装置の実施の形態 1 の構成図である。

図 2 は、上記実施の形態のハード構成を示す外観図及び上記実施の形態で得られた記録媒体の再生装置の外観図である。

- 20 図 3 は、上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の一例を示す図である。

図 4 は、上記実施の形態の一次記録媒体にダウンロードされた音楽データのデータ構造の一例を示す図である。

- 25 図 5 は、上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の他の一例を示す図である。

図 6 は、上記実施の形態の動作を説明するフローチャートのその 1 である。

図 7 は、上記実施の形態の動作を説明するフローチャートのその 2 である。

図 8 は、本発明に係るデジタルデータ記録装置の実施の形態 2 の構成図である。

図 9 は、上記実施の形態の情報提供者が提供するデジタル信号を記録する際
5 の表示部に表示される情報を示す図である。

図 10 は、上記実施の形態の動作を示すフローチャートである。

図 11 は、本発明に係るデジタルデータ記録装置の実施の形態 3 の構成図である。

図 12 は、上記実施の形態の情報提供者が提供するデジタル信号の属性情報
10 のデータ構造を示す図である。

図 13 は、上記実施の形態の動作を示すフローチャートのその 1 である。

図 14 は、上記実施の形態の動作を示すフローチャートのその 2 である。

図 15 は、本発明に係るデジタルデータ記録装置の実施の形態 4 の構成図である。

図 16 は、本発明に係るデジタルデータ記録装置の実施の形態 6 の構成図で
15 ある。

図 17 は、上記実施の形態のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

図 18 は、上記実施の形態の記録媒体に記録される管理情報のデータ構造の一
20 例を示す図である。

図 19 は、上記実施の形態の動作を説明するフローチャートである。

図 20 は、上記実施の形態で記録された記録媒体を再生するデジタルデータ再生装置の構成図である。

図 21 は、上記デジタルデータ再生装置の動作を説明するフローチャートであ
25 る。

図 22 は、本発明に係るデジタルデータ記録装置の実施の形態 7 の構成図で

ある。

図 2 3 は、上記実施の形態のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

図 2 4 は、上記実施の形態の動作を説明するフローチャートである。

- 5 図 2 5 は、上記実施の形態 7 の変形例のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

発明を実施するための最良の形態

- 以下、本発明に係るデジタルデータ記録装置の実施の形態について図面を用
10 いて説明する。

(実施の形態 1)

- 図 1 は、本発明に係るデジタルデータ記録装置の実施の形態 1 の構成図である。
このデジタルデータ記録装置は、データ送受信部 1 0 0 と、受付部 1 0 1 と、
一次記録媒体 1 0 2 と、データ取出部 1 0 3 と、判定部 1 0 4 と、復号化部群 1
15 0 5 と、暗号方式指示部 1 0 9 と、暗号化部群 1 1 0 と、二次記録媒体 1 1 4 と、
記録部 1 1 5 と、固有情報取得部 1 1 6 と、指示受付部 1 1 7 と、課金部 1 1 8
とを備えている。

- なお、このデジタルデータ記録装置の二次記録媒体 1 1 4 と記録部 1 1 5 以
外は、一般には図 2 に示すように P C (パーソナルコンピュータ) 2 0 1 で実現
20 され、記録部 1 1 5 は、例えば D V D (Digital Versatile Disc)-RAM ドライブ
2 0 2 で、二次記録媒体 1 1 4 は、D V D -RAM ディスク 2 0 3 でそれぞれ実
現される。

- このデジタルデータ記録装置は、インターネットを介して配信される暗号化
されたデジタルデータである音楽データを受信し、一次記録媒体 1 0 2 にダウ
25 ンロードした後、復号化部群 1 0 5 でデジタルデータを復号化し、暗号化部群
1 1 0 で再度暗号化したデジタルデータとして、記録部 1 1 5 で二次記録媒体

114に記録する。

なお、本実施の形態では、電子音楽配信について説明するけれども、デジタルデータの種類は、音楽データに限るものではなく、映像データ、文字データあるいはこれらの組み合わせでもよい。

- 5 データ送受信部100は、モデムと制御ソフトで実現される通信部であり、電話回線を通じて情報提供者のホストコンピュータ（図示せず）に接続される。受付部101で受け付けられた希望する曲の購入要求をデータ取出部103を介して通知されると、ホストコンピュータに送信する。インターネットを介して、ホストコンピュータから購入要求に従い配信される音楽データをダウンロードし、
- 10 一次記録媒体102に記録する。また、曲を購入したときに生じる課金情報をホストコンピュータに送信する。

- ここで、情報提供者が提供する情報について説明する。情報提供者は、曲販売のサイト、すなわち自社のホームページを開設しており、曲名、価格などユーザの購入時に必要な情報、あるいは購買意欲をかきたてる情報を提供している。ユーザは、これらの情報提供者が提供する情報に基づいて、好みの曲を購入する。
- 15 ユーザは、これらの情報提供者が提供する情報に基づいて、好みの曲を購入する。

- 図3は、情報提供者が提供する情報、すなわち曲販売用のホームページの一例を示すものである。表示される情報としては、曲名301、歌手名302、収録時間303、価格304などの内容からなる。ここで、曲名301、歌手名302は、それぞれ、個々の音楽データの曲名、歌手名を表す情報である。収録時間303は、個々の曲の収録時間（再生時間）を示し、価格304は、個々の曲の
- 20 303は、個々の曲の収録時間（再生時間）を示し、価格304は、個々の曲の販売価格を示している。これらの情報をもとに、ユーザは受付部101を通じて好みの曲を選択し、購入要求を通知することができる。もちろん、情報提供者が提供する情報は、図3に示すように、文字情報に限られるものではなく、ジャケットピクチャのような画像や、試聴用の音楽データであってもよいことは言うまでもない。
- 25 でもない。

受付部101は、キーボードやマウス等からなり、PCの表示画面に表示され

た図 3 に示した情報を見たユーザから音楽データの購入要求を受け付ける。受け付けた曲の購入要求は、データ取出部 103 を介して、データ送受信部 100 に通知される。

5 一次記録媒体 102 は、一般には PC のハードディスク等で実現され、データ送受信部 100 で受信された暗号化されたデジタルデータである音楽データを記憶している。また、一次記録媒体のセキュアな領域には、課金部 118 によって、ダウンロードされた音楽データを二次記録媒体 114 に記録したとき、例えば暗号化した課金データが記録される。

10 図 4 は、一次記録媒体 102 に記憶されているダウンロードした音楽データ、すなわち情報提供者が提供する音楽データのデータ構造の一例を示すものである。情報提供者が提供する音楽データは、大きく音楽データの曲名や歌手名、価格などの情報である属性情報 401 と、音楽データそのものである曲データ部 402 とから構成される。

属性情報 401 は、ISRC 情報 403、曲名 404、歌手名 405、価格 406、15 情報提供者名 407、暗号形式 408 から構成される。以下、これらの属性情報について説明する。

ISRC(International Standard Recording Code)情報 403 は、音楽データごとに割り当てられる固有の情報であって、国コード (2 つの ASCII 文字)、オーナーコード (3 つの ASCII 文字)、記録年 (数字 2 桁)、シリアル番号 (数字 20 桁) で構成される。曲名 404、歌手名 405 は、それぞれ音楽データの曲名、歌手名を表す文字情報である。価格 406 は、音楽データの価格を表す情報である。なお、本実施の形態では、ダウンロードした音楽データをデジタルデータ記録装置を用いて、二次記録媒体に記録したときに請求される金額を示している。

25 情報提供者名 407 は、音楽データの提供者名、あるいは著作権者名を示す情報である。つまり、ユーザが本デジタルデータ記録装置を用いて音楽データを記録したときに課金し、その金額をどの業者に振り分ければよいのかを示す情報

である。

暗号形式 408 は、ダウンロードした音楽データがどの暗号形式で暗号化されているかを示す情報である。すなわち音楽データは、情報提供者ごとに異なる暗号方式で暗号化されている。例えば、情報提供者 A、情報提供者 B、情報提供者 C が音楽データを提供する場合、情報提供者 A の提供する音楽データは A 方式で暗号化されており、情報提供者 B の提供する音楽データは B 方式で暗号化されており、情報提供者 C の提供する音楽データは C 方式で暗号化されている。なお、本実施の形態では、情報提供者の提供する情報が、さまざまな形式で暗号化されている場合に、それを記録した二次記録媒体 114 を再生装置で著作権の保護を図りつつ、容易に解読できる暗号形式に変換することが発明の主たる目的であり、暗号化のアルゴリズムの詳細な説明については省略する。

また、属性情報 401 においては、価格 406、情報提供者名 407 は改竄されると情報提供者が不利益を被るおそれがあるため、必要に応じて暗号化されている。

データ取出部 103 は、暗号方式指示部 109 からデジタルデータの取り出し指示を受けると、一次記録媒体 102 から、まず属性情報 401 を取り出し、属性情報 401 を課金部 118 に通知する。また、属性情報 401 中の暗号形式 408 の情報は、判定部 104 に通知する。なお、属性情報 401 中、価格 406 等が暗号化されているときは、復号化部群 105 によって、復号化してから課金部 118 に通知する。さらに一次記録媒体 102 から曲データ部 402 を取り出し、判定部 104 に出力する。データ取出部 103 で取り出されたデータは、すでに述べたように、情報提供者ごとに異なる暗号方式で暗号化されている。

判定部 104 は、データ取出部 103 から通知された暗号形式 408 の情報に基づいて、復号化部群 105 のいずれの復号化部に音楽データを出力するか判定する。

復号化部群 105 は、n 個の復号化部よりなり、第 1 復号化部 106 は A 方

式で暗号化されたデジタルデータを復号し、第2復号化部107はB方式で暗号化されたデジタルデータを復号し、第n復号化部108はN方式で暗号化されたデジタルデータを復号する。各復号化部106～108は、情報提供者ごとの復号モジュールからなっている。

- 5 例えば、判定部104に通知された暗号形式408の情報がB方式であれば、判定部104は、音楽データの曲データ部402のデジタルデータを第2復号化部107に出力し、復号する。第2復号化部107は、入力されたデジタルデータを復号して、暗号方式指示部109に出力する。

- 10 第1から第n復号化部106～108のいずれかにより暗号化されたデータを復号する際、復号鍵が必要であればデータ送受信部100でデータの暗号方式に応じた復号鍵を入手し、データを復号化する。このようにして情報提供者ごとに異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化する。

- 15 暗号方式指示部109は、指示受付部117から暗号方式の種類 of 指示を受けているときは、その指示に従った固有情報の取得を固有情報取得部116に指示する。固有情報取得部116から指示した固有情報の通知を受けたときは、データ取出部103に音楽データの取り出しを指示する。固有情報取得部116から指示に従った固有情報を取得できない旨の通知を受けたときには、表示部（図示せず）に指示された暗号方式の種類では暗号化できない旨を表示させる。また、
- 20 指示受付部117から暗号方式の種類 of 指示を受けていないときには、固有情報取得部116に二次記録媒体114の属性に従った固有情報の取得を指示する。固有情報取得部116から固有情報又は固有情報を取得できない旨を通知されると、データ取出部103に音楽データの取り出しを指示する。固有情報を取得できない旨の通知を受けたときには、乱数を発生する。

- 25 暗号方式指示部109は、指示受付部117から暗号方式の指示を受け付けているときは、その指示に応じた一の暗号化部を選び、復号化部群105のいずれ

かの復号化部 106、107、…、108 から復号されたデジタルデータの入力を受けると、固有情報取得部 116 から通知された固有情報とともに、復号されたデジタルデータを通知する。

- また、暗号方式指示部 109 は、指示受付部 117 から指示を受け付けていないときには、固有情報取得部 116 から通知された固有情報の種類に従い、一の暗号化部を選び、復号化部群 105 のいずれかの復号化部 106～108 から復号されたデジタルデータの入力を受けると、固有情報とともにデジタルデータを通知する。固有情報取得部 116 から固有情報を取得できない旨の通知を受けているとき、発生させた乱数とともに、一の暗号化部にデジタルデータを通知する。

- 暗号化部群 110 は、 n 個の暗号化部 111、112、…、113 からなる。各暗号化部 111、112、…、113 は、異なる種類の暗号鍵によって、通知されたデジタルデータを暗号化する。例えば、第 1 暗号化部 111 は、二次記録媒体 114 の固有の識別情報を基に作成される暗号鍵で暗号化する。第 2 暗号化部 112 は、二次記録媒体 114 を再生する再生装置（図示せず）の固有の識別情報を基に作成される暗号鍵で暗号化する。第 n 暗号化部 113 は、乱数を基に作成される暗号鍵で暗号化する。暗号化部 111～113 で用いられる各暗号鍵のデータサイズは、一次記録媒体 102 に記憶されている暗号化されたデジタルデータの暗号鍵のデータサイズよりも小さく設定される。

- 二次記録媒体 114 に記録される暗号化されたデジタルデータの暗号鍵のデータサイズが小さいことは、このデジタルデータを解読する際の困難性が低いことを意味する。したがって、二次記録媒体 114 を再生する再生装置でのデジタルデータの復号化に要する構成が簡単化されることになり、再生装置のコスト減につながる。

- 例えば、指示受付部 117 からの指示がないときに、暗号方式指示部 109 が固有情報取得部 116 から二次記録媒体の識別情報の通知を受けているときには、

第1暗号化部111に二次記録媒体の識別情報を通知する。第1暗号化部111は、その識別情報を基に暗号鍵を作成し、暗号方式指示部109から通知された音楽データの属性情報401の暗号形式408を書き換えるとともに、曲データ部402を、生成した暗号鍵で暗号化する。暗号化したデジタルデータを記録部115に通知する。

また、暗号方式指示部109は、指示受付部117から二次記録媒体114を再生する再生装置（図示せず）の固有情報による暗号化の指示を受けると、固有情報取得部116に再生装置の固有の識別情報を取得するよう指示する。固有情報取得部116から再生装置の固有の識別情報を通知されると、その識別情報と復号化部群105から通知された復号されたデジタルデータとを第2暗号化部112に通知する。

第2暗号化部112は、暗号方式指示部109から通知された識別情報を基に暗号鍵を生成し、生成した暗号鍵でデジタルデータを暗号化して記録部115に通知する。この際、音楽データの属性情報401の暗号形式408の内容を書き換えるのは、指示受付部117から指示を受け付けないときと同様である。

二次記録媒体114は、例えば図2に示したDVD-RAMディスク、MD、再生装置（図示せず）の機種により埋め込み型あるいは取り外し可能な型の小型の半導体メモリ等からなり、暗号化部群110で暗号化された音楽データが記録部115によって記録される。例えば、DVD-RAMディスク203にデジタルデータが記録されていれば、図2に示すように、DVD-Audioプレーヤ204にDVD-RAMディスク203を挿入して音楽を聴取することができる。

記録部115は、例えば、図2に示したDVD-RAMドライブ202で実現され、暗号化部群110から通知されたデジタルデータを二次記録媒体114に記録する。また、記録が終了すると、その旨、課金部118に通知する。

固有情報取得部116は、暗号方式指示部109から二次記録媒体114の固有の識別情報の取得を指示されたときには、例えば、DVD-RAMの場合は

BCA(Burst Cutting Area)に書かれている情報を読み出し、通知する。なお、この二次記録媒体 1 1 4 の固有の識別情報は、媒体ごとにユニークであり、通常ディスクの製造時に記録される情報であって、ユーザの通常の操作では読み出されたり、書き換えることができない。

- 5 したがって、この識別情報を基に暗号鍵を生成して、この暗号鍵で暗号化されたデジタルデータが DVD-RAM ディスクに記録されるので、万一悪意を持ったユーザがビットコピー可能なツールを用いて DVD-RAM ディスクの内容を複製し、再生しようとしても、復号鍵の基になる情報が異なるため、正常に復号化することができない。この結果、音楽データの著作権を確実に保護することができ
- 10 きる。

- また、暗号方式指示部 1 0 9 から二次記録媒体 1 1 4 が装着された再生装置(図示せず)の固有の識別情報の取得を指示されたときには、固有情報取得部 1 1 6 は、再生装置の識別情報を読み出し、暗号方式指示部 1 0 9 に通知する。この再生装置の固有の識別情報も再生装置の製造時に付される装置ごとのユニーク
- 15 な識別情報であるので、ユーザの通常の操作では読み出されたり、書き換えられたりすることはできない。したがって、この識別情報を基に暗号化された場合も、特定の再生装置でしか再生することができない。

- なお、固有情報取得部 1 1 6 は、暗号方式指示部 1 0 9 から指示された固有の識別情報を取得できないとき、即ち、二次記録媒体 1 1 4 又は再生装置に識別情報
- 20 が付されていない場合には、指示された種類の固有の識別情報を取得できない旨を暗号方式指示部 1 0 9 に通知する。

- 固有情報取得部 1 1 6 は、暗号方式指示部 1 0 9 から固有情報の種類の指示を受けずに、固有情報の取得の指示を受けると、二次記録媒体 1 1 4 が DVD-RAM ディスクなどの再生装置から取り外し可能なものであるか、それとも、小型の半導体メモリのような再生装置に埋め込まれた取り外し不可能ものであるかを判断し、取り外し可能なものであれば、その二次記録媒体 1 1 4 の固有の識別
- 25

情報を読み出し、暗号方式指示部 1 0 9 に二次記録媒体 1 1 4 の識別情報を通知し、取り外し不可能なものであれば、再生装置の識別情報を読み出し、同様に再生装置の識別情報を通知する。識別情報を取得できないときは、その旨を暗号方式指示部 1 0 9 に通知する。

- 5 指示受付部 1 1 7 は、P C のキーボードやマウスで実現され、ユーザから暗号方式の種類の指示を受け付け、暗号方式指示部 1 0 9 に通知する。

先に述べた図 3 に示すホームページの情報では、販売価格は 1 通りしかなかったけれども、図 5 に示すようなホームページの内容であれば、価格 (1) 5 0 1 、価格 (2) 5 0 2 の 2 通りの販売価格が示されている。

- 10 価格 (1) 5 0 1 は、二次記録媒体 1 1 4 の固有の識別情報を基にデジタルデータを暗号化して記録するときの価格を示しており、価格 (2) 5 0 2 は、二次記録媒体 1 1 4 を再生する再生装置の固有の識別情報を基にデジタルデータを暗号化して記録するときの価格を示している。なお、これらの 2 種類の価格は、情報提供者側でそれぞれ個別に自由に設定可能である。

- 15 ユーザは、指示受付部 1 1 7 から二次記録媒体 1 1 4 の利用形態に応じて、図 5 に示す曲情報あるいはその価格情報を参照して好みの暗号形態でデジタルデータを暗号化することを指示することができる。例えば、特定の再生装置でのみ再生するとき、即ち、他の再生装置で二次記録媒体 1 1 4 を再生しないときには、再生装置の固有の識別情報を基に暗号化することを指示する。図 5 に示すように
- 20 再生装置の識別情報を基に暗号化するほうが、価格 (2) 5 0 2 に示すように一般的に安価である。これは、他の再生装置で再生することができないので、二次記録媒体 1 1 4 の固有の識別情報を基に暗号化するよりも自由度が低いからである。ユーザは、自由に再生装置を選んで再生したいときには、二次記録媒体 1 1 4 の識別情報を基に暗号化するよう指示すればよい。

- 25 なお、指示受付部 1 1 7 と上述の受付部 1 0 1 とは、一体として構成されているけれども、説明上、2 つの構成要素として説明した。

課金部 118 は、データ取出部 103 から音楽データの属性情報 401 の通知を受け、記憶している。記録部 115 から暗号化されたデジタルデータを二次記録媒体 114 に記録した旨の通知を受けると、属性情報中の価格 406 を参照して課金額を決定し、一次記録媒体 102 のセキュアな領域に属性情報 401 とともに課金情報として書き込む。

なお、価格 406 が図 5 に示したように価格 (1) 501、価格 (2) 502 のように複数あるときは、暗号方式指示部 109 から通知された第 1 から第 n 暗号化部 111 ~ 113 のいずれが利用されたかに従い課金額を決定する。

次に、本実施の形態の動作を図 6、図 7 のフローチャートを用いて説明する。

10 先ず、受付部 101 はユーザからのホームページ表示の要求を受け、データ送受信部 100 が音楽データを提供する情報提供者が開設するホームページにアクセスし、データ取出部 103 によって表示部 (図性せず) にホームページ (図 3、図 5 参照) を表示させる (S602)。

次に、データ取出部 103 は、受付部 101 からユーザの希望する音楽データの購入指示を待ち、指定された音楽データの配信を受けるようデータ送受信部 15 100 に指示する (S604)。データ送受信部 100 は、音楽データを受信すると、一次記録媒体 102 にダウンロードする (S606)。

ユーザは、ホームページの表示をみて、暗号方式の種類を二次記録媒体 114 の利用形態に応じて、指示受付部 117 から入力する。

20 暗号方式指示部 109 は、指示受付部 117 から暗号方式の種類 of 指示を通知されたか否か判断し (S608)、通知されたときは、指示された暗号方式の種類に用いる固有情報の取得を固有情報取得部 116 に指示する (S610)。固有情報取得部 116 から指示された固有情報を取得できない旨の通知を受けたか否かを判断し (S612)、その旨の通知を受けたときは、指示された暗号方式 25 の種類では暗号化できない旨を表示部 (図示せず) に表示させ (S614)、処理を終了する。指示した種類の固有情報の通知を受けたときには、データ取出部

103にデジタルデータの取り出しを指示する。

データ取出部103は、一次記録媒体102に記録されている音楽データを取り出す(S616)。

5 S608において、暗号方式指示部109は、指示受付部117から指示を通知されないと判断したとき、固有情報取得部116に固有情報の種類を指定しないで、固有情報の取得を指示する(S618)。

固有情報取得部116は、二次記録媒体114の属性(再生装置(図示せず)に装着された二次記録媒体114が取り外し可能か不可能か)を判断し、取り外し可能な二次記録媒体114のときは二次記録媒体114の識別情報を取得し、
10 取り外し不可能な二次記録媒体114のときは再生装置の識別情報を取得する(S620)。

暗号方式指示部109は、固有情報取得部116から取得された固有(識別)情報又は、固有情報を取得できなかったときはその旨の通知を受けると(S622)、データ取出部103にデジタルデータの取り出しを指示し、S616に
15 移る。

次に、判定部104は、データ取出部103で取り出された音楽データの属性情報401中の暗号形式408を参照して、復号化部群105のいずれの復号化部106~108で復号するかを判定する(S702)。

判定部104で判定された一の復号化部は、判定部104を介して入力された
20 デジタルデータを復号化し、復号したデジタルデータを暗号方式指示部109に出力する(S704)。

暗号方式指示部109は、既に固有情報取得部116から通知されている固有情報(取得できない旨の情報も含む)に従い、暗号化部群110の一の暗号化部を選び、固有情報(取得できない旨の情報に対しては発生した乱数)と復号化さ
25 れたデジタルデータとを通知する(S706)。

暗号方式指示部109から通知を受けた一の暗号化部は、固有(識別)情報に

基づいて暗号鍵を生成し（乱数の通知に対しては乱数に基づいて暗号鍵を生成し）、デジタルデータを暗号化する。この際、属性情報 4 0 1 のうち暗号形式 4 0 8 の内容も書き換えられる（S 7 0 8）。

記録部 1 1 5 は、第 1 ～ 第 n 暗号化部 1 1 1 ～ 1 1 3 のいずれかから通知されたデジタルデータを二次記録媒体 1 1 4 に記録し（S 7 1 0）、記録が終了すると課金部 1 1 8 に通知する。

課金部 1 1 8 は、記録部 1 1 5 から通知を受けると、データ取出部 1 0 3 から通知されている価格 4 0 6 等に従い課金額を決定し、課金情報を一次記録媒体 1 0 2 に記録して（S 7 1 2）処理を終了する。

10 上記実施の形態では、復号化部群 1 0 5 は、情報提供者ごとの復号モジュール（復号化部）からなるものとしたけれども、復号化部群は、音楽データの品質、例えば 2 4 ビットの L P C M (Liner Pulse Code Modulation)、M P 3 (Moving Picture Experts Group 1 Audio Layer 3) 等のデジタルデータ、に応じて各復号化部を設けてもよい。高品質の 2 4 ビットの L P C M は、解読の困難性の高い
15 暗号化されたデジタルデータとし、通常品質の M P 3 は解読の困難性の低い暗号化されたデジタルデータとしておき、第 1 復号化部は 2 4 ビットの L P C M のデジタルデータを復号し、第 2 復号化部は M P 3 のデジタルデータを復号するようにしてもよい。

上記実施の形態では、暗号化部群 1 1 0 は、固有情報の種類で各暗号化部を設けたけれども、上述した品質に対応して、第 1 復号化部で復号化されたデジタルデータは第 1 暗号化部で暗号化し、第 2 復号化部で復号化されたデジタルデータは第 2 暗号化部で暗号化し、第 n 復号化部で復号化されたデジタルデータは第 n 暗号化部で暗号化するようにしてもよい。この場合、第 1 暗号化部で暗号化に用いる暗号鍵のデータサイズは、第 2 暗号化部のそれよりも大きく、第 2 暗号化部のそれは第 n 暗号化部のそれよりも大きく設定する。そして、課金部は、
25 デジタルデータの復号化がされた復号化部と復号化されたデジタルデータを

再暗号化部がされた暗号化部とによって課金額を決定する。このようにすることによって、高品質の音楽データの方がより著作権の保護を確実なものとする事ができる。また、この際、価格についても情報提供者は高品質の音楽データに高価格を設定することができる。

5 なお、上記実施の形態のデジタルデータ記録装置は、図 1 にその構成図を示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムをコンピュータ読み取り可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないデジタルデータ記録装置に摘要して著作権の保護機能を有する装置とすることができる。

10 また、本実施の形態では、デジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらず音楽データ、あるいは、属性情報のみをいったんユーザの PC 内の一次記録媒体 102 に記録しておき、一次記録媒体 102 に記録されているデジタルデータに対して購入手続きを行う形態も考えられる。

15 また、本実施の形態では、属性情報 401 は曲データ 402 と別個に記述するとして説明を行ったが、いわゆる Water Mark（電子すかし）の形式で曲データ 402 のデジタルデータ中に埋め込むことも可能である。

20 また、本実施の形態において、復号化部群 105 と暗号化部群 110 との間の暗号方式指示部 109 を介してのデータ入出力に関しては特に言及はしていないが、セキュリティ上、認証を行ってデータを送信するか、あるいは復号化部群 105、暗号方式指示部 109 及び暗号化部群 110 を 1 つのチップで実現する、といった方法で復号化されたデータの漏洩を防ぐようにしてもよい。

25 また、課金情報を記録するときには、一次記録媒体 102 中のセキュアな領域に記録するとして説明を行ったが、課金情報に関しては、一次記録媒体 102 とは別の IC カードなどの記録媒体を設け、これに記録することが可能である。

本実施の形態では、課金のタイミングについては、説明を省略したが、例えば、

デジタルデータを二次記録媒体 1 1 4 に記録するときに必ずホストコンピュータと接続していなければいけないとするか、課金額が一定の金額に達するとホストコンピュータに自動的に接続するか、あるいは、課金情報記録後、一定の日時が経過すると自動的にホストコンピュータに接続する、としてもよい。

- 5 更に、本実施の形態では、情報提供者が提供する情報を音声情報として説明したが、これに限るものではなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報との組み合わせたものなどでもよいことはもちろんである。

(実施の形態 2)

- 10 図 8 は、本発明に係わるデジタルデータ記録装置の実施の形態 2 の構成図である。このデジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部 2 1 0 1、一次記録媒体 2 1 0 2、データ取出部 2 1 0 3、暗号方式判定部 2 1 0 4、第 1 の復号化部 2 1 0 5、第 2 の復号化部 2 1 0 6、第 3 の復号化部 2 1 0 7、暗号化部 2 1 0 8、記録部 2 1 0 9、二次記録媒体 2 1 1 0、入力部 2 1 1 1、表示部 2 1 1 2、記録媒体固有情報取得部 2 1 1 3 を備える。また、復号化部群 2 1 1 5 は、第 1 の復号化部 2 1 0 5、第 2 の復号化部 2 1 0 6、第 3 の復号化部 2 1 0 7 から構成されるが、復号化部は 3 つに限るものではなく、ここでは、複数の復号化部から構成されることを示している。

- 20 なお、本実施の形態では、以後、記録対象となるデータを音楽データであるとし、音楽データはインターネットを通じて配信されるものとする。また、情報提供者ごとに異なる暗号方式でデータを暗号化しているものとする。

- 25 情報提供者は、曲名、価格、コピー制御情報など（以後、属性情報と称する）購入時に必要な情報、あるいは購買意欲をかきたてる情報を音楽データに重畳または音楽データから分離して提供するものとするが、本実施の形態では、属性情報を音楽データから分離して提供する形態について説明する。

データ送受信部 2 1 0 1 は、モデムで実現される通信部であり、電話回線を通

- じて提供者のホストコンピュータ（図示せず）に接続される。まず、ユーザは情報提供者が提供する属性情報を取得する。データ送受信部 2101 により取得した属性情報は、一次記録媒体 2102 に記録され、その一部または全部が表示部 2112 に表示される。図 9 は、表示部 2112 に表示される情報の一例を示す
- 5 ものである。表示される情報としては、曲名 2201、曲名コード 2202、歌手名 2203、データ入手先 2204 などの内容からなる。ここで、曲名 2201、歌手名 2203 は、それぞれ音楽データに対する曲名、歌手名を表す情報である。曲名コード 2202 は、音楽データを他の音楽データと識別するための識別子であり、例えば I S R C (International Standard Recording Code)
- 10 情報が付される。これらの情報をもとに、ユーザは入力部 2111 を通じて好みの曲を選択し、購入要求を通知することができる。データ入手先 2204 は、本実施の形態では該当する曲が記録されている U R L (Uniform Resource Locator) 情報とする。もちろん、曲名コード 2202 に I S R C 情報が付されていれば、曲名コード 2202 からデータ入手先を特定することも可能である。
- 15 入力部 2111 は、マウス、キーボード等から実現され、ユーザからの曲の購入の指示、すなわち記録指示を受け付け、データ送受信部 2101 に通知する。ユーザは表示部 2112 に表示された情報を元に、マウスでその曲名等をクリックして音楽データの記録を指示する。

- 入力部 2111 から音楽データの記録指示があると、データ送受信部 2101
- 20 から電話回線を通じて提供者のホストコンピュータから記録要求のあった曲をダウンロードする。この際に、属性情報中の U R L 情報をもとに曲データの位置を特定する。ダウンロードされたデータはいったん一次記録媒体 2102 に記録される。

- 一次記録媒体 2102 は、一般にはパソコンのハードディスクであって、ユー
- 25 ザが購入を希望した音楽データを暗号化されたまま記録する。したがって以後の動作に関しては、必ずしも常に提供者のホストコンピュータと接続している必要

はない。

- データ取出部 2103 は、一次記録媒体 2102 から記録対象となる音楽データを
取り出す。このとき、ユーザは表示部 2112 に表示される図 9 に示した情
報と同程度の情報をもとに、二次記録媒体 2110 へ記録する音楽データを入力
5 部 2111 を通じて選択する。データ取出部 2103 で取り出されたデータは、
各情報提供者ごとの暗号方式で暗号化されている。このため、適当な復号方式で
復号することを暗号方式判定部 2104 により判定する。具体的には、ディジタ
ルデータのヘッダ部に暗号方式を識別できる情報を付加して送信する、属性情報
に暗号方式を記述しておく、などの方法が考えられ、これらの値に応じて暗号方
10 式を判定する。

- 第 1 の復号化部 2105、第 2 の復号化部 2106、第 3 の復号化部 2107
は、各情報提供者ごとの復号方式が存在していることを示すものであって、必ず
しも 3 つに限られるわけではない。暗号方式判定部 2104 により適当な復号化
部を選択し、復号化部により暗号化されたデータを復号する。このとき、例えば
15 暗号方式判定部 2104 で取得したデータの暗号方式に応じた復号鍵を入手また
は生成し、復号化部はこの復号鍵をもとにデータを復号化する。したがって、異
なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されて
いるデータを復号化することになる。

- 次に、暗号化部 2108 にて復号化されたデータの暗号化を行うが、ここでは、
20 記録媒体固有の固有情報を暗号鍵情報として暗号化を行うこととする。なお、記
録媒体固有情報をもとに暗号化を行う一の方法については、特開平 5-2578
16 公報に開示されているので、ここでは詳しい説明は省略する。

記録媒体固有情報取得部 2113 は、暗号化部 2108 からの指示に従い、二次
記録媒体 2110 から固有情報を取り出し、暗号化部 2108 へ伝達する。

- 25 暗号化部 2108 は、記録媒体固有情報取得部 2113 で取得した固有情報を
暗号鍵として、暗号化する。

ここで、二次記録媒体 2 1 1 0 固有の情報について説明する。

二次記録媒体 2 1 1 0 は、媒体ごとの固有の識別情報を持っている。これは例えば DVD-RAM (Digital Versatile Disc Random Access Memory) の場合、BCA (Burst Cutting Area) に書かれた情報に相当する。この情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持ったユーザがビットコピー可能なツールを用いてディスクの内容を複製したとしても、復号鍵のもとになる情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

10 記録部 2 1 0 9 は、暗号化されたデータを二次記録媒体 2 1 1 0 に記録する。

以上のように構成されたデジタルデータ記録装置について、以後図 1 0 のフローチャートを用いてその動作を説明する。

まず、データ送受信部 2 1 0 1 は、属性情報をダウンロードし (S 2 3 0 1)、ユーザからのデジタルデータの記録指示を待ち (S 2 3 0 2)、指示されたデジタルデータをダウンロードし、一次記録媒体 2 1 0 2 に記録する (S 2 3 0 3)。次に、ダウンロードしたデータの暗号方式を判定し、適当な復号化部 2 1 0 5 ~ 2 1 0 7 へ復号化を指示する (S 2 3 0 4)。復号化部 2 1 0 5 ~ 2 1 0 7 により復号化する (S 2 3 0 5)。暗号化部 2 1 0 8 は、復号化されたデータが入力されると、記録媒体固有情報取得部 2 1 1 3 から二次記録媒体 2 1 1 0 の固有情報を取得する (S 2 3 0 6)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部 2 1 0 8 はデータを暗号化する (S 2 3 0 7)。記録部 2 1 0 9 は、暗号化されたデータを二次記録媒体 2 1 1 0 に記録し (S 2 3 0 8)、処理を終了する。

25 以上で、本発明の実施の形態 2 のデジタルデータ記録装置に関する説明を終わる。

次に、本発明の実施の形態 3 のデジタルデータ記録装置に関する説明を行う。

(実施の形態 3)

図 1 1 は、本発明に係わるデジタルデータ記録装置の実施の形態 3 の構成図である。このデジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部 2 1 0 1、一次記録媒体 2 1 0 2、データ取出部 2 1 0 3、暗号方式判定部 2 1 0 4、復号化部群 2 1 1 5、属性情報取得部 2 4 0 1、コピー制御情報検出判定部 2 4 0 2、コピー制御情報変換部 2 4 0 3、課金情報算出部 2 4 0 4、暗号化部 2 1 0 8、記録部 2 1 0 9、二次記録媒体 2 1 1 0、入力部 2 1 1 1、表示部 2 1 1 2、記録媒体固有情報取得部 2 1 1 3 を備える。

なお、実施の形態 3 では、実施の形態 2 のデジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。

まず、本実施の形態において、記録対象となるデータの属性情報が図 1 2 の通りであるとする。図 1 2 に示す属性情報は、図 9 に示す属性情報に加えて、コピー制御情報 2 5 0 1、課金情報 2 5 0 2 等の情報がある。ここで、コピー制御情報 2 5 0 1 は、コピーが許可されている世代数、あるいは回数の情報からなる。例えば世代数に関しては、「無制限にコピー可」、「1 世代だけコピー可（孫コピー禁止）」、「コピー禁止」等の値を取る。一方、回数に関しては、コピー許可されている回数のことで、0 以上の整数値を取りうる。例えば「孫コピー不可」は、二次記録媒体 2 1 1 0 にデジタルデータを記録後、二次記録媒体 2 1 1 0 中のデータをもとにコピーすることを許可しないことを意味する。「無制限に許可」は、特に制限しないことを意味する。「2 回コピー可」など、コピーの回数の情報が含まれる場合は、二次記録媒体 2 1 1 0 に記録できる回数を意味する。

属性情報取得部 2 4 0 1 は、一次記録媒体 2 1 0 2 から、再生すべきデータに対応する属性情報を取得する。ここでは、コピー制御情報と課金情報を取り出す。なお、属性情報は著作権保護情報や課金情報を含むので、一次記録媒体 2 1 0 2 中のセキュアな領域に記録して、ユーザの通常の操作ではアクセスできないこと

が望ましい。

コピー制御情報検出判定部 2402 は、属性情報中のコピー制御情報を取り出し、以後のコピーが許可されているかどうか、許可されているとすればその世代数、あるいは回数の情報を取得する。

- 5 コピー制御情報検出判定部 2403 は、コピーが許可されている場合、コピー制御情報を必要に応じて書き換える。例えば、孫コピーが禁止されているときは、コピー制御情報の値を以後のコピーを禁止するように変更し、コピー許可回数が制限されているときは、許可回数から「1」減じた値に変更する。

- 10 ここで重要となるのは、コピー許可回数が設定されているとき、一般に、一次記録媒体 2102 に記録されたデータを何回二次記録媒体 2110 にコピーさせるかという数値であるため、コピー制御情報の書き換え対象となるのは、一次記録媒体 2102 中に記録されているデータである。したがって、一次記録媒体 2102 中に記録されている。コピー許可回数を「1」減じた値に変換し、二次記録媒体 2110 に記録すべきコピー許可回数は 0 として記録する。

- 15 課金情報算出部 2404 は、属性情報取得部 2401 で取得した属性情報から該当する曲の課金情報を取得し、これをもとに課金額を算出し、一次記録媒体 2102 中のセキュアな領域に記録する。

以上のように構成されたデジタルデータ記録装置について、以下、図 13 および図 14 のフローチャートを用いてその動作を説明する。

- 20 まず、データ送受信部 2101 は、属性情報をダウンロードし (S2601)、ユーザからのデジタルデータの記録指示を待ち (S2602)、指示されたデジタルデータをダウンロードし、一次記録媒体 2102 に記録する (S2603)。次に、記録対象となるデータの属性情報を属性情報取得部 2401 により取得する (S2604)。コピー制御情報判定部 2402 により属性情報中のコピー制御情報を判定し、コピーが許可されているかどうかを判定する (S2605)。コピーが許可されているときは、コピーが許可されている世代、回数の情
- 25

報を取得し、必要に応じてコピー制御情報変換部 2403 で書き換える (S2606)。コピーが許可されていない場合は、以後の処理を中断する (S2607)。次に暗号方式を判定し、復号化群 2115 中の適当な復号化部へ復号化を指示する (S2608)。復号化部 2105 ~ 2107 により復号化を行う (S2609)。復号化が終わると、属性情報取得部 2401 で取得した属性情報中の課金情報から適切な課金額を算出する (S2610)。

暗号化部 2108 は、復号化されたデータが入力されると、記録媒体固有情報取得部 2113 から二次記録媒体 2110 の固有情報を取得する (S2611)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部 2108 はデータを暗号化する (S2612)。記録部 2109 は、暗号化されたデータを二次記録媒体 2110 に記録し (S2613)、処理を終了する。

以上で、本発明の実施の形態 3 に関する説明を終わる。

(実施の形態 4)

次に、本発明に係わるデジタルデータ記録装置の実施の形態 4 について説明する。このデジタルデータ記録装置は、実施の形態 2 とほぼ同一であるが、固有情報取得送出部 2803、記録部 2109、二次記録媒体 2110 が第 2 のデジタルデータ記録装置内にある点と、暗号鍵の情報のみが異なる。図 15 は、本発明に係わるデジタルデータ記録装置の実施の形態 4 の構成図である。このデジタルデータ記録装置は、第 1 のデジタルデータ記録装置 2800 と、第 2 のデジタルデータ記録装置 2801 とからなる。

第 1 のデジタルデータ記録装置 2800 は、データ送受信部 2101、一次記録媒体 2102、データ取出部 2103、暗号方式判定部 2104、復号化部群 2115、暗号化部 2108、入力部 2111、表示部 2112、固有情報取得部 2802 備える。

第 2 のデジタルデータ記録装置 2801 は、固有情報取得送出部 2803、記録部 2109、二次記録媒体 2110 を備える。

なお、実施の形態 4 では、実施の形態 2 のデジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。

- 暗号化部 2 1 0 8 へ復号化部群 2 1 1 5 にて復号されたデータが入力されると、
- 5 記録媒体固有情報取得部 2 8 0 2 は、第 2 のデジタルデータ記録装置 2 8 0 1 中の固有情報取得送出部 2 8 0 3 へ固有情報の送出要求を出す。固有情報取得送出部 2 8 0 3 は、第 2 のデジタルデータ記録装置 2 8 0 1 に装着されている二次記録媒体 2 1 1 0 の固有識別情報、あるいは第 2 のデジタルデータ記録装置 2 8 0 1 固有の識別情報、あるいはその両方を取得し、固有情報取得部 8 0 2 へ
- 10 送出する。

- 暗号化部 2 1 0 8 では、第 2 のデジタルデータ記録装置 2 8 0 1 に装着されている二次記録媒体 1 1 0 の固有識別情報、あるいは第 2 のデジタルデータ記録装置 8 0 1 固有の識別情報、あるいは、二次記録媒体 2 1 1 0 の固有識別情報と第 2 のデジタルデータ記録装置 2 8 0 1 固有の識別情報の組み合わせの情報
- 15 を暗号鍵の一部としてデータを暗号化し、第 2 のデジタルデータ記録装置 2 8 0 1 へ出力する。第 2 のデジタルデータ記録装置 2 8 0 1 中の記録部 2 1 0 9 は暗号化されたデータを二次記録媒体 2 1 1 0 へ記録する。

- なお、固有情報取得送出部 2 8 0 3 で取得送出する固有情報であるが、二次記録媒体 2 1 1 0 が第 2 のデジタルデータ記録装置 2 8 0 1 に固定的に設けられているときは、装置固有の識別情報とし、二次記録媒体 2 1 1 0 が着脱自在に設けられているときは、二次記録媒体 2 1 1 0 固有の固有情報、あるいは二次記録媒体 2 1 1 0 の固有識別情報と第 2 のデジタルデータ記録装置 2 8 0 1 固有の識別情報の組み合わせの情報とすることにより、より柔軟な暗号方式を使用することが可能になる。

- 25 以上で、実施の形態 4 の説明を終わる。

(実施の形態 5)

次に、本発明に係わるデジタルデータ記録装置の実施の形態 5 について説明する。このデジタルデータ記録装置は、実施の形態 2、3 および 4 とほぼ同一である。ここでは、実施の形態 4 の説明に用いた構成図、図 15 を用いて説明する。相違点は、二次記録媒体 2110 に応じた暗号形式を採用し、記録すること
5 である。つまり、DVD-RAM と半導体メモリとでは取り扱うデータの最小単位、暗号化データを書きこむデータ量の単位の単位が異なるため、固有情報取得部 2802 は、固有情報取得送出部 2803 から、媒体の情報も取得して、最適なデータの単位で暗号化を行なうことになる。このため、暗号化部 2108 が複数存在し、適切な暗号化部へ固有情報ならびに媒体情報も伝達するものである。以上
10 より、DVD-RAM に限らず、半導体メモリ、IC カード、ハードディスク等を二次記録媒体 2110 として使用することが可能となる。

以上で、実施の形態 5 の説明を終わる。

なお、上記実施の形態 2～5 は現状において最善の効果が期待できるシステム例として説明したにすぎない。本発明は、その要旨を逸脱しない範囲で実施変更
15 することができる。具体的には以下に示すような変更実施が可能である。

また、実施の形態 2～5 では、デジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらずいったんユーザの PC 内の一次記録媒体 2102 に記録しておき、一次記録媒体 2102 に記録されているデジタルデータに対して購入
20 手続きを行う形態も考えられる。

また、実施の形態 2～5 では、コピー制御情報を属性情報に記述するとして説明を行なったが、いわゆる Water Mark (電子すかし) の形式でデジタルデータ中に埋め込むことも可能である。

また、課金情報を記録するときには、一次記録媒体 2102 中のセキュアな領域に記録するとして説明を行なったが、課金情報に関しては、一次記録媒体 2102 とは別の IC カードなどの記録媒体を設け、これに記録することが可能であ
25

る。

また、実施の形態 2～5 では、情報提供者が提供する情報を音声情報として説明したが、これに限るものでなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報の組み合わせたものなどでもよいことはもちろんである。

(実施の形態 6)

図 16 は、本発明に係るデジタルデータ記録装置の実施の形態 6 の構成図である。

このデジタルデータ記録装置は、通信部 3101 と、記録媒体 3102 と、
10 受信データ記録判定部 3103 と、表示部 3104 と、入力操作部 3105 と、
記録媒体固有情報取得部 3106 と、暗号化部 3107 と、記録部 3108 と、
課金情報記録部 3109 と、課金情報記録媒体 3110 と、課金部 3111 とを
備えており、PC で実現される。

通信部 3101 は、モデムで実現され、電話回線を介してデータ提供者のホス
15 トコンピュータ（図示せず）及び課金センタ（図示せず）に接続される。ホス
トコンピュータからデジタルデータとその属性情報とを受信すると、受信データ
記録判定部 3103 に通知する。

また、通信部 3101 は、課金センタから利用料の問い合わせがあると、その
旨課金部 3111 に通知し、課金部 3111 から課金情報の通知を受けると、電
20 話回線を介して、課金センタに課金情報を通知する。

本実施の形態では、データ提供者が提供するデジタルデータを音楽データであるとして説明する。データ提供者は、提供する音楽データを必要に応じて暗号化したデジタルデータとし、デジタルデータには、情報識別子が付されている。情報識別子は、曲名コードであり、他の音楽と識別するためのものである。

25 また、デジタルデータには、属性情報が付加されている。属性情報は、デジタルデータの利用料金等を示すものであり、どの情報提供者から提供された情

報であるかを示す情報も含まれている。

図 17 は、属性情報の内容の一例を示す図である。属性情報 3201 には、デジタルデータの曲名 3202、演奏者（歌手）3203、曲名コード 3204、記録料金 3205、1 回あたりの再生料金 3206、再生可能回数 3207、暗号状態 3208、コピー許可 3209 等の項目の内容が含まれる。

ここで、曲名 3202、演奏者 3203 は、表示部 3104 に表示して、ユーザがコピー（複製）をするか否かを指示する判断資料となるものである。曲名コード 3204 は、音楽データを他の音楽データと識別するための識別子であり、曲ごとにユニークなものであり、例えば I S R C（International Standard Recording Code）が付される。なお、このコードは国コード（2 つの ASCII 文字）、オーナーコード（3 つの ASCII 文字）、記録年（数字 2 桁）、シリアル番号（数字 5 桁）で構成されている。

記録料金 3205、1 回あたり再生料金 3206、再生可能回数 3207 等は、課金基準データを構成し、いずれもその音楽データの利用料金を算定する為の情報である。

記録料金 3205 は、通信部 3101 で受信されたデジタルデータを記録媒体 3102 に記録する際の料金である。1 回あたりの再生料金 3206 は、記録媒体 3102 に記録されたデジタルデータの再生 1 回あたりの料金を示している。再生可能回数 3207 は、記録媒体 3102 に記録されたデジタルデータの再生が許容される回数を示している。「100 回」と記録されているときには、100 回に限り再生できることを示している。また、再生回数が一定回数以上になると、その後の料金が不要となる買い取り形式の設定も可能である。

暗号状態 3208 は、暗号有無フラグであり、通信部 3101 で受信されたデジタルデータが暗号化されているか否かを示すものである。

コピー許可 3209 は、記録許可フラグであり、ユーザ側で記録する、即ち、記録媒体 3102 に受信された音楽データを記録することを許可するか否かを示

す情報である。「1回のみ可」とは、1度だけ記録することが許可され、「許可」は、何度でも記録することが許可されていることを示している。

5 なお、本発明は、受信された音楽データを記録媒体 3 1 0 2 に記録（複製）し、再生するときの音楽の著作権保護を図ることを主目的としたものであるので、この音楽データをリアルタイムに聴取するだけが許可されている場合についての説明は、簡単にする。この場合は、コピー許可 3 2 0 9 は、「不可」とされている。このデジタルデータ記録装置には、復号化部と出力部とがその構成から省略されているけれども、通信部 3 1 0 1 で受信されたデジタルデータは復号化部で復号され、出力部から音楽が出力される。この際、課金基準データには、聴取料
10 金が含まれている。

記録媒体 3 1 0 2 は、書き換え可能な記憶部材からなり、装置本体に着脱可能に取り付けられており、例えば、DVD-RAM 等で構成される。

記録媒体 3 1 0 2 の書き換え不能なセキュアな領域には、記録媒体 3 1 0 2 の固有情報が予め記録されている。

15 また、記録媒体 3 1 0 2 には、記録部 3 1 0 8 によって、暗号化部 3 1 0 7 で暗号化されたデジタルデータが記録される。

更に、記録媒体 3 1 0 2 には、記録されたデジタルデータの管理情報と属性情報とが記録部 3 1 0 8 によって記録されている。

受信データ記録判定部 3 1 0 3 は、通信部 3 1 0 1 からデジタルデータとその属性情報 3 2 0 1 との通知を受けると、その属性情報 3 2 0 1 を最初に通知されたとき記憶し、属性情報のうち、曲名 3 2 0 2、演奏者 3 2 0 3、記録料金 3 2 0 5、1 回あたり再生料金 3 2 0 6 等を表示部 3 1 0 4 に表示させ、デジタルデータを暗号化部 3 1 0 7 に通知する。
20

入力操作部 3 1 0 5 からコピー（複製）指示を受けると、指示された音楽の曲
25 名コード 3 2 0 4 のデジタルデータのコピーが可能か否かを属性情報 3 2 0 1 のコピー許可 3 2 0 9 を見て判断する。コピーが許可であれば、記録媒体固有情

報取得部 3106 に記録媒体 3102 の固有情報を取得するよう指示する。また、暗号化部 3107 に曲名コード 3204 と暗号状態 3208 を通知する。

コピーが不可であれば、表示部 3104 にその旨を表示させる。

- 受信データ記録判定部 3103 は、記録部 3108 からコピー終了の通知を受けると、記憶している属性情報 3201 の項目、コピー許可 3209 を書き換える。即ち、コピー許可 3209 が「1 回のみ」とされているときには「コピー不可」に、「何回のみ可」と数字が記録されているときには「1」を減じた数字にそれぞれ書き換える。なお、この属性情報 3201 を記憶する記憶領域は、EEPROM 内に設けられており、このデジタルデータ記録装置の電源がオフされた場合でも記憶内容は消失されない。

- 例えば、暗号化部 3107 に曲名コード 3204 の「song01」を通知した後に、記録部 3108 からコピー終了の通知を受けると、「song01」に対応する項目、コピー許可 3209 を「1 回のみ可」から「コピー不可」に書き換える。このようにすることによってデータ提供者の有する権利が侵されることを防止できる。

表示部 3104 は、液晶ディスプレイや CRT 等からなり、受信データ記録判定部 3103 の制御により、デジタルデータである音楽データの曲名等の表示や、コピーができない旨の表示をする。

- 入力操作部 3105 は、マウス等からなり、ユーザのコピー指示を受け付け、受信データ記録判定部 3103 に通知する。ユーザは、表示部 3104 に表示された曲名や演奏者の表示を見て、記録媒体 3102 にその音楽をダウンロードしようとするとき、マウスでその曲名等をクリックして、その音楽のコピーを指示する。

- 記録媒体固有情報取得部 3106 は、受信データ記録判定部 3103 から固有情報の取得指示を受けると、記録媒体 3102 のセキュアな領域に記録されている固有情報を読み出し、暗号化部 3107 に通知する。

暗号化部 3 1 0 7 は、記録媒体固有情報取得部 3 1 0 6 から通知された固有情報を基に暗号鍵を作成する。受信データ記録判定部 3 1 0 3 から通知されたデジタルデータを作成した暗号鍵を用いて暗号化したデジタルデータを作成し、記録部 3 1 0 8 に通知する。

- 5 なお、受信データ記録判定部 3 1 0 3 から通知されたデジタルデータが暗号化されている旨の通知を受けている場合には、そのデジタルデータを復号化しておいてもよいし、そのままの状態でもよい。

- 例えば、記録媒体 3 1 0 2 に記録すべきデジタルデータ dataA を受信データ記録判定部 3 1 0 3 から通知された場合に、記録媒体 3 1 0 2 の固有情報を基に暗号鍵 KM を作成すると、暗号化したデジタルデータ E (KM, dataA) を作成する。他の記録媒体にデジタルデータ dataA を記録する場合には、その他の記録媒体の固有情報を基に暗号鍵 K'M を作成したときは、暗号化したデジタルデータ E は、E (K'M, dataA) となる。

- ここで、デジタルデータの暗号化の技術については、特開平 5 - 2 5 7 8 1
15 6 号公報に記載されている。

記録部 3 1 0 8 は、暗号化部 3 1 0 7 から通知された暗号化されたデジタルデータを記録媒体 3 1 0 2 に記録する。この際、記録媒体 3 1 0 2 に記録したデジタルデータの管理情報を作成して、記録媒体 3 1 0 2 に記録する。

- 図 1 8 は、管理情報の一例を示す図である。管理情報 3 3 0 1 には、記録した
20 デジタルデータの識別子である曲名コード 3 2 0 4 と、記録媒体 3 1 0 2 に記録されたデジタルデータの記録開始アドレス 3 3 0 2、記録終了アドレス 3 3 0 3 とが対応して記録される。

記録媒体 3 1 0 2 に記録されたデジタルデータを再生する際、この管理情報 3 3 0 1 が参照される。

- 25 また、記録部 3 1 0 8 は、記録媒体 3 1 0 2 に暗号化されたデジタルデータ及び管理情報の記録が終了すると、受信データ記録判定部 3 1 0 3 に記憶されて

いる記録したデジタルデータに対応する属性情報 3 2 0 1 を読み出し、記録媒体 3 1 0 2 に書き込む。更に、受信データ記録判定部 3 1 0 3 にコピー終了の通知をする。また、課金情報記録部 3 1 0 9 に、記録したデジタルデータの曲名コードを通知する。

- 5 課金情報記録部 3 1 0 9 は、記録部 3 1 0 8 から曲名コード 3 2 0 4 の通知を受けると、受信データ記録判定部 3 1 0 3 に記憶されている曲名コード 3 2 0 4 に対応する属性情報 3 2 0 1 の記録料金 3 2 0 5 を読み出し、記録料金が有料のときは、課金情報記録媒体 3 1 1 0 にその曲名コードと記録料金と記録日時等を課金情報として記録する。

- 10 課金情報記録媒体 3 1 1 0 は、RAMカード等からなり、記録媒体 3 1 0 2 にダウンロードしたデジタルデータの課金情報が課金情報記録部 3 1 0 9 によって記録される。

- 課金部 3 1 1 1 は、通信部 3 1 0 1 を介して課金センタ（図示せず）からの利用料の問い合わせがあると、課金情報記録媒体 3 1 1 0 に記録されている未決済
15 の課金情報を読み出し、通信部 3 1 0 1 に通知する。通知が終了すると、課金センタに通知済（決済）のフラグを課金情報記録媒体 3 1 1 0 に記録する。

次に、本実施の形態の動作を図 1 9 のフローチャートを用いて説明する。

- 先ず、受信データ記録判定部 3 1 0 3 は、ユーザからデジタルデータの記録指示を待ち（S 3 4 0 2）、指示されたデジタルデータのコピーが許可されて
20 いるか否かを属性情報 2 0 1 を見て判断する（S 3 4 0 4）。否のときは、コピーが許可されていない旨を表示部 3 1 0 4 に表示させ（S 3 4 0 6）、処理を終了する。

- コピーが許可されているときは、記録媒体固有情報取得部 3 1 0 6 は、記録媒体 3 1 0 2 のセキュアな領域に記録されている記録媒体 3 1 0 2 の固有情報を取得し、暗号化部 3 1 0 7 に通知する（S 3 4 0 8）。
25

暗号化部 3 1 0 7 は、固有情報を基に暗号鍵を作成し、デジタルデータを暗

号化する (S 3 4 1 0)。

記録部 3 1 0 8 は、暗号化されたデジタルデータを記録媒体 3 1 0 2 に記録する (S 3 4 1 2)。

次に、課金情報記録部 3 1 0 9 は、記録されたデジタルデータの記録料金が
5 有料か否かを判断する (S 3 4 1 4)。無料であれば、処理を終了し、有料であれば、課金情報記録媒体 1 1 0 に課金情報を記録して (S 3 4 1 6)、処理を終了する。

図 2 0 は、上述のデジタルデータ記録装置で記録媒体 3 1 0 2 に記録されたデジタルデータの再生装置の構成図である。

10 このデジタルデータ再生装置は、記録媒体 3 1 0 2 と、入力操作部 3 5 0 1 と、再生情報読出部 3 5 0 2 と、表示部 3 5 0 3 と、記録媒体固有情報取得部 3 5 0 4 と、復号化部 3 5 0 5 と、再生部 3 5 0 6 と、課金情報記録部 3 5 0 7 と、課金情報記録媒体 3 5 0 8 とを備えている。

記録媒体 3 1 0 2 は、上記デジタルデータ記録装置で暗号化されたデジタル
15 ルデータと管理情報 3 3 0 1 と属性情報 3 2 0 1 とが記録された DVD-RAM を識別する識別子である固有情報が記録されている。

入力操作部 3 5 0 1 は、ユーザから再生開始の指示を受けると、再生情報読出部 3 5 0 2 に初期起動の指示を与える。ユーザから曲名の指示を受けると、その曲名を再生情報読出部 3 5 0 2 に通知する。なお、初期起動の指示の他に記録媒
20 体 3 1 0 2 がこのデジタルデータ再生装置に挿入されたときにも自動再生モードの指示が再生情報読出部 3 5 0 2 に与えられる。

再生情報読出部 3 5 0 2 は、入力操作部 3 5 0 1 から初期起動の指示を受けると、記録媒体 3 1 0 2 に記録されている属性情報 3 2 0 1 を読み出し、その項目である曲名 3 2 0 2 及び演奏者 3 2 0 3 の一覧を表示部 3 5 0 3 に表示させる。

25 また、入力操作部 3 5 0 1 から曲名の指示又は、自動再生モードの指示を受けると、属性情報 3 2 0 1 の対応する再生可能回数 3 2 0 7 が「1」以上であるか

- 否かを判断する。再生可能回数 3 2 0 7 が「1」以上であれば、その曲名コード 3 2 0 4 を読み出し、管理情報 3 3 0 1 の記録開始アドレスから記録終了アドレスまでに記録された暗号化されたデジタルデータを読み出し、復号化部 3 5 0 5 に通知する。この際、記録媒体固有情報取得部 3 5 0 4 に固有情報を取得する
- 5 よう指示するとともに、課金情報記録部 3 5 0 7 に、曲名コード 3 2 0 4 と 1 回あたりの再生料金 3 2 0 6 とを通知する。更にデジタルデータの読み出しが終了すると、属性情報 3 2 0 1 の項目である再生可能回数 3 2 0 7 の数を「1」減じた数に書き換える。なお、再生可能回数 3 2 0 7 が「無限」の場合には、そのままにする。
- 10 再生情報読出部 3 5 0 2 は、再生可能回数が「1」未満であると判断したとき、表示部 3 5 0 3 に再生可能回数が越えた旨を表示させる。
- 表示部 3 5 0 3 は、液晶ディスプレイ等からなり、再生情報読出部 3 5 0 2 で読み出された曲名等を一覧表示する。また、再生可能回数を超えてのユーザからの曲名指定に対して、再生可能回数が越えた旨を表示する。
- 15 記録媒体固有情報取得部 3 5 0 4 は、再生情報読出部 3 5 0 2 から固有情報の取得を指示されると、記録媒体 3 1 0 2 のセキュアな領域から記録媒体 3 1 0 2 の識別子である固有情報を取得し、復号化部 3 5 0 5 に通知する。
- 復号化部 3 5 0 5 は、記録媒体固有情報取得部 3 5 0 4 から固有情報の通知と、再生情報読出部 3 5 0 2 から暗号化されたデジタルデータの通知とを受けると、
- 20 固有情報を基に復号鍵を作成して、暗号化されたデジタルデータを復号し、復号化したデジタルデータを再生部 3 5 0 6 に通知する。
- 再生部 3 5 0 6 は、復号化部 3 5 0 5 からデジタルデータの通知を受けると、デコードして音楽を再生する。音楽の再生を終了すると課金情報記録部 3 5 0 7 に再生終了を通知する。
- 25 課金情報記録部 3 5 0 7 は、再生部 3 5 0 6 から再生終了の通知を受けると、再生情報読出部 3 5 0 2 から通知されている曲名コード 3 2 0 4 と 1 回あたりの

再生料金 3 2 0 6 と再生日時とを課金情報として課金情報記録媒体 3 5 0 8 に記録する。なお、1 回あたりの再生料金 3 2 0 6 が有料でなければ、記録はしない。

課金情報記録媒体 3 5 0 8 は、RAM カード等からなり、課金情報を課金情報記録部 3 5 0 7 によって記録される。

- 5 次に、このデジタルデータ再生装置の動作を図 2 1 に示すフローチャートを用いて説明する。

先ず、ユーザは、再生開始を入力操作部 3 5 0 1 のリモコン等を用いて指示し、表示部 3 5 0 3 に表示された曲名を指定する。再生情報読出部 3 5 0 2 は、音楽の再生要求であるとし (S 3 6 0 2)、指定された曲名の再生可能回数が「1」

- 10 以上であるか否かを属性情報 3 2 0 1 をみて判断する (S 3 6 0 4)。再生可能回数が「1」未満であれば、表示部 3 5 0 3 に再生可能回数を超えた旨を表示させ (S 3 6 0 6)、処理を終了する。

- 15 再生可能回数が「1」以上の場合には、再生情報読出部 3 5 0 2 は、記録媒体 3 1 0 2 から暗号化されたデジタルデータを読み出し、復号化部 3 5 0 5 に通知する (S 3 6 0 8)。

記録媒体固有情報取得部 3 5 0 4 は、記録媒体 3 1 0 2 から固有情報を取得して復号化部 3 5 0 5 に通知する (S 3 6 1 0)。

復号化部 3 5 0 5 は、固有情報を復号鍵として暗号化されたデジタルデータを復号化する (S 3 6 1 2)。

- 20 再生部 3 5 0 6 は、デジタルデータをデコードして音楽を再生出力する (S 3 6 1 4)。

課金情報記録部 3 5 0 7 は、再生料金が有料であるか否かを判断し (S 3 6 1 6)、無料のときは何もせずに、有料のときは、課金情報を課金情報記録媒体 3 5 0 8 に記録して (S 3 6 1 8)、処理を終了する。

- 25 (実施の形態 7)

図 2 2 は、本発明に係るデジタルデータ記録装置の実施の形態 7 の構成図で

ある。このデジタルデータ記録装置は、第1デジタルデータ記録装置3700と第2デジタルデータ記録再生装置3710とからなる。

第1デジタルデータ記録装置3700は、第1記録媒体3701と、通信部3101と、受信データ1次記録判定部3702と、表示部3104と、入力操作部3105と、1次記録部3703と、受信データ読出判定部3704と、固有情報取得部3705と、暗号化部3706と、課金情報記録部3109と、課金情報記録媒体3110と、課金部3111とを備えており、PCで実現される。

第2デジタルデータ記録再生装置3710は、固有情報取得送出部3707と、2次記録部3708と、第2記録媒体3709と、入力操作部3501と、再生情報読出部3502と、表示部3503と、復号化部3505と、再生部3506と、課金情報記録部3507と、課金情報記録媒体3508とを備えている。

なお、上記実施の形態6のデジタルデータ記録装置及びデジタルデータ再生装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、
15 本実施の形態固有の部分についてのみ説明する。

まず、第1デジタルデータ記録装置3700について説明する。上記実施の形態6のデジタルデータ記録装置と異なるのは、第1記録媒体3701が本装置に固定的に設けられ、この第1記録媒体3701に記録されたデジタルデータが2次記録のために暗号化されて出力されることである。

20 第1記録媒体3701は、本装置3700内に固定的に設けられたハードディスク等の書き込み可能な記録部材からなる。第1記録媒体3701には、通信部3101で受信された音楽データであるデジタルデータとその管理情報とが1次記録部3703によって書き込まれる。

受信データ1次記録判定部3702は、通信部3101で受信されたデジタルデータに付された属性データをEEPROM内に設けられた記憶領域に書き込む。本実施の形態で受信される属性情報の一例を図23に示す。属性情報380

1 は、上記実施の形態 6 の属性情報 3 2 0 1 と 2 次記録料金 3 8 0 2 が記録されていることと、コピー許可（1 次） 3 8 0 3 と（2 次） 3 8 0 4 との記録の許可回数が示されていることとが異なる。

5 また、曲名コード「song05」の「曲 E」では、コピーが 1 次、2 次ともに不許可であり、リアルタイムの聴取のみが許可された音楽であることを示している。

受信データ 1 次記録判定部 3 7 0 2 は、ユーザからある音楽の 2 次記録の指示を受けると、先ず 1 次記録が許可されているか否かを属性情報 3 8 0 1 の項目コピー許可（1 次） 3 8 0 3 を見て判断する。許可されていないときは、表示部 3 1 0 4 に不許可である旨を表示させる。許可されているときは、指示された音楽
10 のデジタルデータを 1 次記録部 3 7 0 3 に通知する。他の機能は、上記実施の形態 6 の受信データ記録判定部 3 1 0 3 と同様である。

1 次記録部 3 7 0 3 は、通知されたデジタルデータを第 1 記録媒体 3 7 0 1 に記録する。この際、管理情報を書き込むのは、上記実施の形態 6 の記録部 3 1 0 8 と同様である。なお、上記実施の形態 6 では、記録媒体 3 1 0 2 の固有情報を基に暗号鍵が作成され、デジタルデータが暗号化されていたけれども、本実施
15 の形態では、第 1 記録媒体 3 7 0 1 が取外され、他の装置で利用されることがないので暗号化されない。

また、1 次記録部 3 7 0 3 は、第 1 記録媒体 3 7 0 1 へのデジタルデータの記録が終了すると、受信データ読出判定部 3 7 0 4 に記録した曲名コード 3 8 0
20 5 を通知する。

受信データ読出判定部 3 7 0 4 は、1 次記録部 3 7 0 3 から曲名コード 3 8 0 5 の通知を受けると、その音楽の 2 次記録が許可されているか否かを、受信データ 1 次記録判定部 3 7 0 2 の属性情報 3 8 0 1 中のコピー許可（2 次） 3 8 0 4 を見て判断する。許可されていないとき、又は、許可回数が「1」以上でないとき
25 には、表示部 3 1 0 4 に 2 次記録が許可されていない旨を表示させる。

受信データ読出判定部 3 7 0 4 は、2 次記録が許可されているときには、管理

情報（図 18 参照）を見て、第 1 記録媒体 3701 に記録されている通知された曲名コードのデジタルデータを読み出して暗号化部 3706 に通知するとともに、固有情報取得部 3705 に固有情報を取得するよう指示する。

また、受信データ読出判定部 3704 は、デジタルデータの読み出しが完了すると、受信データ 1 次記録判定部 3702 に記憶されている属性情報 3801 のコピー許可（2 次）3804 の回数から「1」減じた数に書き換える。例えば「1 回のみ可」であれば「不許可」に書き換え、「許可」だけであれば、回数に制限がないので、そのまま書き換えは行わない。

なお、受信データ読出判定部 3704 は、暗号化部 3706 にデジタルデータの通知の後に、受信データ 1 次記録判定部 3702 に記憶されている属性情報を読み出して通知する。

固有情報取得部 3705 は、受信データ読出判定部 3704 から固有情報を取得するよう指示されると、第 1 デジタルデータ記録装置 3700 に接続されている第 2 デジタルデータ記録再生装置 3710 の固有情報取得送出部 3707 に、固有情報の送出を要求する。固有情報取得送出部 3707 から固有情報の通知を受けると、暗号化部 3706 に固有情報を通知する。

暗号化部 3706 は、固有情報取得部 3705 から通知された固有情報を基に暗号鍵を作成し、受信データ読出判定部 3704 から通知されたデジタルデータを暗号化して第 2 デジタルデータ記録再生装置 3710 の 2 次記録部 3708 に送出する。この暗号化されたデジタルデータの送出の後に、通知された属性情報も送出する。

次に、第 2 デジタルデータ記録再生装置 3710 について説明する。この第 2 デジタルデータ記録再生装置 3710 は、携帯型の例えばヘッドフォンステレオタイプの装置で実現される。また、第 2 記録媒体 3709 がこの装置 3710 から着脱自在の半導体メモリの IC カード等から構成されている。

固有情報取得送出部 3707 は、第 1 デジタルデータ記録装置 3700 の固

有情報取得部 3705 から固有情報の送出要求を受けると、第 2 記録媒体 3709 に予め記録されている第 2 記録媒体固有の媒体識別情報と、この装置 3710 固有の機器識別情報とを取得して、固有情報取得部 3705 に通知する。また、再生情報読出部 3502 から固有情報の通知指示を受けると、復号化部 3505

5 に媒体識別情報と機器識別情報とを通知する。

2 次記録部 3708 は、第 1 デジタルデータ記録装置 3700 の暗号化部 3706 から暗号化されたデジタルデータと、属性情報との出力を受けると、第 2 記録媒体 3709 に記録する。併せて、図 18 に示したような管理情報 3301 を記録する。復号化部 3505 は、固有情報取得送出部 3707 から通知され

10 た媒体識別情報と機器識別情報との 2 つの情報を基に復号鍵を作成して、再生情報読出部 3502 から通知された暗号化されたデジタルデータを復号する。なお、その他の構成は、上記実施の形態 6 のデジタルデータ再生装置の構成とほぼ同様である。

次に、第 2 記録媒体 3709 がこの装置 3710 に固定的に設けられた IC カ

15 ード等から構成される場合について述べる。この場合には、第 2 記録媒体 3709 がこの装置 3710 以外で再生されることがないことから固有情報取得送出部 3707 は、媒体識別情報を取得することなく、自ら記憶している機器識別情報を固有情報取得部 3705 に通知する。また、復号化部 3505 にも、機器識別情報を通知する。

20 このように、第 2 デジタルデータ記録再生装置 3710 に設けられた第 2 記録媒体 3709 が着脱自在であるか否かによって、デジタルデータの暗号化の暗号鍵の作成を媒体識別情報と機器識別情報との組合せによるか、機器識別情報だけで行うかを使い分けることができる。このように使い分けることによっても、デジタルデータの不正な複製や不正な再生利用を防止することができる。

25 次に、本実施の形態の動作を図 24 に示すフローチャートを用いて説明する。先ず、受信データ 1 次記録判定部 3702 は、入力操作部 3105 からディジタ

ルデータの２次記録の指示が有るのを待ち（Ｓ３９０２）、デジタルデータの１次記録が許可されているか否かを属性情報３８０１を見て判断する（Ｓ３９０４）。許可されていないときは、その旨を表示部３１０４に表示させて（Ｓ３９０６）、処理を終了する。

- ５ 許可されているときは、受信データ１次記録判定部３７０２は、デジタルデータを１次記録部３７０３に通知する。１次記録部３７０３は、第１記録媒体３７０１にデジタルデータと管理情報とを記録する（Ｓ３９０８）。

次に、課金情報記録部３１０９は、１次記録に対して課金されているか否かを判断し（Ｓ３９１０）、１次コピーが有料の時は課金情報を課金情報記録媒体３１１０に記録する（Ｓ３９１２）。

- 次に、受信データ読出判定部３７０４は、第１記録媒体３７０１に記録されたデジタルデータの２次記録が許可されているか否かを受信データ１次記録判定部３７０２に記憶されている属性情報３８０１を見て判断する（Ｓ３９１４）。許可されていないときは、２次記録が許可されていない旨を表示部３１０４に表示させ（Ｓ３９１６）、処理を終了する。

- 許可されているときは、受信データ読出判定部３７０４は、第１記録媒体３７０１からデジタルデータを読み出し、暗号化部３７０６に通知するとともに、固有情報取得部３７０５に第２デジタルデータ記録再生装置３７１０から固有情報を取得するよう指示する。固有情報取得部３７０５は、固有情報を取得し、暗号化部３７０６に通知する（Ｓ３９１８）。暗号化部３７０６は、通知された固有情報を基に暗号鍵を作成し（Ｓ３９２０）、通知されているデジタルデータを暗号化して第２デジタルデータ記録再生装置３７１０の２次記録部３７０８に出力する。

- ２次記録部３７０８は、通知された暗号化されたデジタルデータと属性情報と管理情報とを第２記録媒体３７０９に記録する（Ｓ３９２２）。

また、課金情報記録部３１０９は、２次記録に対して課金されているか否かを判

断し（S 3 9 2 4）、2次記録が有料のときは、課金情報を課金情報記録媒体 1 1 0 に記録し（S 3 9 2 6）、処理を終了する。

なお、第2デジタルデータ記録再生装置 3 7 1 0 でのデジタルデータの再生動作は、実施の形態 6 のデジタルデータ再生装置の動作とほぼ同様であるの

5 で説明を省略する。

（変形例）

上記実施の形態 7 では、第2記録媒体 3 7 0 9 が着脱自在であるときには、第2デジタル記録再生装置 3 7 1 0 の機器識別情報と、第2記録媒体 3 7 0 9 の媒体識別情報とを組合せた暗号鍵でデジタルデータが暗号化されたけれども、

10 本変形例では、暗号化の形態（媒体識別情報のみに基づいた暗号鍵とするのか媒体識別情報に機器識別情報を組合わせた暗号鍵とするのか）をユーザに指定させ、ユーザの利用形態の自由度を拡大している。即ち、第2デジタルデータ記録再生装置 3 7 1 0 で第2記録媒体 3 7 0 9 に記録された音楽を再生しようとするときには、媒体識別情報及び機器識別情報でデジタルデータを暗号化して記録する

15 るようにし、他のデジタルデータ再生装置（媒体識別情報を復号鍵として暗号化されたデジタルデータを復号化できる装置）で第2記録媒体 3 7 0 9 に記録された音楽を再生しようとするときには、媒体識別情報でデジタルデータを暗号化して記録するようにする。ユーザの利用形態に応じて暗号化の形態を選択できるようにしている。

20 一方、このユーザの利用の自由度に応じて2次記録料金を設定して、著作権の保護を図っている。

以下、本変形例の具体的構成を説明する。なお、本変形例は、図 2 2 に示した第1デジタルデータ記録装置 3 7 0 0 の構成に若干の機能を追加するものであるので、実施の形態 7 の構成図をそのまま利用して、本変形例固有の構成についてのみ説明する。

25

図 2 5 は、受信データ1次記録判定部 3 7 0 2 に記憶されている属性情報 3 1

001の一部を示している。この属性情報31001では、図23に示した属性情報3801の2次記録料金3802と2次記録料金31002との内容が異なる。

2次記録料金31002は、暗号化の暗号鍵が媒体識別情報（媒体ID）31003、機器識別情報（機器ID）31004、媒体識別情報と機器識別情報との組み合わせ31005のいずれであるかによって異なっている。媒体識別情報31003を基に暗号鍵が作成されたものでは、他の装置に第2記録媒体3709を装着して音楽を再生でき、ユーザの自由度が増すことから2次記録料金（2複製利用料金）が機器識別情報31004又は媒体識別情報と機器識別情報との組み合わせ31005を基に暗号鍵が作成されたものよりも高額に設定される。ユーザの利用形態の拡大に応じて複製利用料金を課金できるようにしたものである。

固有情報取得部3705は、固有情報取得送出部3707から機器識別情報と媒体識別情報との通知を受けると、表示部3104に第2記録媒体3709を他の装置で利用するか、第2デジタルデータ記録再生装置3710でのみ利用するかを表示させ、ユーザの選択を待つ。

ユーザは、入力操作部3105より、他の装置を用いるか、第2デジタルデータ記録再生装置3710のみを用いるかを指定する。即ち、暗号鍵を媒体識別情報だけで作成するか、媒体識別情報と機器識別情報との組み合わせで作成するかを指示する。

入力操作部3105は、この指定を固有情報取得部3705と受信データ1次記録判定部3702とに通知する。

受信データ1次記録判定部3702は、入力操作部3105から他の装置を用いるとの通知を受けると、課金情報記録部3109に媒体識別情報31003を暗号鍵とする2次記録料金である旨を、第2デジタルデータ記録再生装置のみを用いるとの通知を受けると、媒体識別情報と機器識別情報との組み合わせ31005を暗号鍵とする2次記録料金である旨を通知する。

固有情報取得部 3705 は、入力操作部 3105 から、他の装置を用いる旨の通知を受けると、暗号化部 3706 に媒体識別情報のみを通知する。また、第 2 デジタルデータ記録再生装置 3710 でのみ用いる旨の通知を受けると、同様に媒体識別情報と機器識別情報とを通知する。

- 5 課金情報記録部 3109 は、暗号化部 3706 から暗号化されたデジタルデータを 2 次記録部 3708 に送出した旨の通知を受けると、受信データ 1 次記録判定部 3702 から通知されている属性情報 31001 の 2 次記録料金 31002 を見て、課金情報記録媒体 3110 に課金情報を記録する。

- 10 なお、本変形例において、第 2 記録媒体が着脱自在の DVD-RAM であるときには、上記実施の形態 6 と同様、DVD-RAM 固有の識別情報のみを基に暗号鍵を作成し、デジタルデータを暗号化して記録するようにできるのは勿論である。

また、本変形例の動作は、上記実施の形態 7 の動作と基本的に異なるところがないのでその説明は省略する。

- 15 なお、上記実施の形態 6、7 及び変形例において、課金情報記録媒体 3110、3508 は例えば IC カードにより実現し、デジタルデータの記録や再生時に IC カードをセットしなければ動作しないとすることも可能である。

- 20 また、上記実施の形態 6、7 及び変形例では、通信部 3110 で受信されるデジタルデータが音楽データであるとして説明したけれども、これに限ることはなく、映像データ、音声データ、文字データやこれらの組合せであってもよいのは勿論である。

- 25 上記実施の形態 6 と実施の形態 7 と変形例のデジタルデータ記録装置及び再生装置並びにデジタルデータ記録再生装置は、図 16、図 20 及び図 22 にその構成図を示したけれども、各構成要素の機能を発揮するプログラムをコンピュータ読取可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないデジタルデータ記録再生装置に適用して著作権の保護機能を有する装置とすることができる。

産業上の利用可能性

以上のように、本発明に係るデジタルデータ記録装置は、著作権保護を図り、再生装置の低コスト化を実現でき、種々の方式で暗号化されて電子配信されるデ

- 5 デジタルデータの記録装置として有用であり、特に電子音楽配信される音楽データの記録装置として最適である。

請 求 の 範 囲

1. デジタルデータを記録媒体に記録するデジタルデータ記録装置において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信手段と、
- 5 前記通信手段により受信された暗号化デジタルデータを復号する復号化手段と、
- 複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでデジタルデータを暗号化する暗号化手段と、
- 10 前記暗号化手段により暗号化されたデジタルデータを前記記録媒体に記録する記録手段と、
- 前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、
- 前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたデジタルデータを再暗号化させることを特徴とするデジタルデータ記録装置。
- 15 2. 前記記録媒体に記録されたデジタルデータは、再生装置により再生され、
- 前記暗号化手段は、
- 前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化
- 20 化する第1暗号化部と、
- 前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第2暗号化部とを有し、
- 前記制御手段は、
- 前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前
- 25 記第1暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第2暗号化部によりデジタルデータの暗号化を行わせることを特徴とする

請求の範囲第 1 項に記載のデジタルデータ記録装置。

3. 前記デジタルデータ記録装置は、更に、

前記デジタルネットワークを介して課金処理を行う課金手段を備え、

5 前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求の範囲第 1 項に記載のデジタルデータ記録装置。

4. 前記記録媒体に記録されたデジタルデータは、再生装置により再生され、

10 前記暗号化手段は、

前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 1 暗号化部と、

前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 2 暗号化部とを有し、

15 前記制御手段は、

前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第 1 暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第 2 暗号化部によりデジタルデータの暗号化を行わせることを特徴とする請求の範囲第 3 項に記載のデジタルデータ記録装置。

20

5. 前記制御手段は、

前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化デジタルデータを、前記復号化手段により復号化することを禁止することを特徴とする請求の範囲第 4 項に記載のデジタルデータ記録装置。

25

6. 前記暗号化手段の有する複数の暗号化部による暗号化されたデジタルデー

タは、前記通信手段により受信されたデジタルデータの暗号化に比べいずれもセキュリティレベルが低いことを特徴とする請求の範囲第 1 項記載のデジタルデータ記録装置。

- 5 7. 前記通信手段により受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、

前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたデジタルデータをそれぞれ復
10 号化し、

前記制御手段は、前記通信手段により受信された暗号化デジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化デジタルデータを復号化するように前記復号化手段を制御することを特徴とする請求の範囲第 1 項に記載のデジタルデータ記録装
15 置。

8. 前記デジタルデータ記録装置は、更に、

前記デジタルネットワークを介して課金処理を行う課金手段を備え、

- 前記制御手段は、受信した暗号化デジタルデータに対し、復号化を行う前記
20 復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求の範囲第 7 項に記載のデジタルデータ記録装置。

9. デジタルデータを記録媒体に記録するデジタルデータ記録方法において、
25 暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、

- 5 前記暗号化ステップにより暗号化されたデジタルデータを前記記録媒体に記録する記録ステップとを有することを特徴とするデジタルデータ記録方法。

- 10 10. 前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、

複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

- 15 前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することを特徴とする請求の範囲第9項に記載のデジタルデータ記録方法。

11. デジタルデータを第1記録媒体に記録するデジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、

- 20 暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、

- 25 前記暗号化ステップにより暗号化されたデジタルデータを前記第1記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラム

を記録したコンピュータ読み取り可能な記録媒体。

12. 前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータ

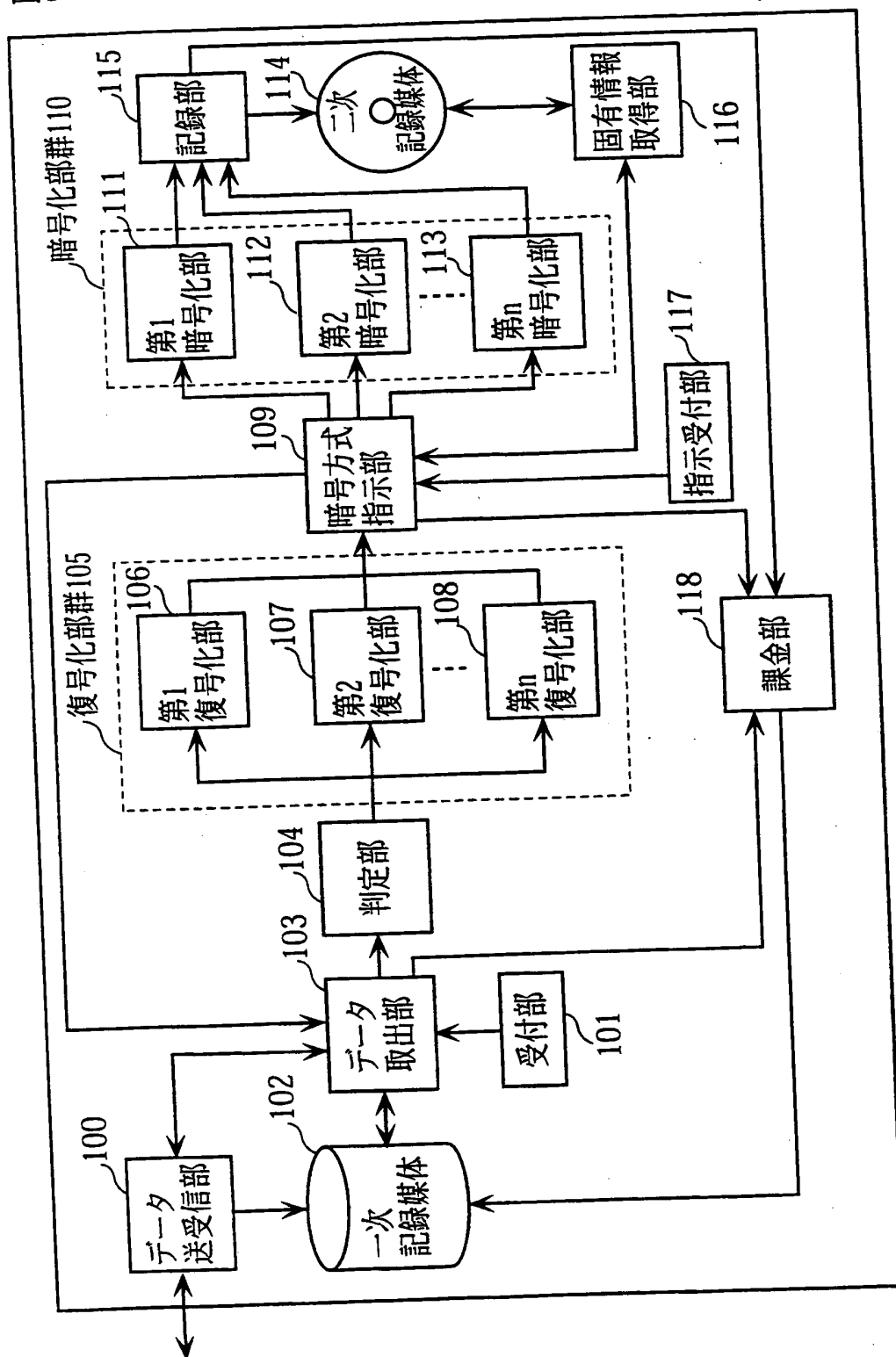
5 は当該データの暗号化方式を示す属性情報を含み、

複数の暗号化方式からい一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求の範

10 囲第11項に記載のコンピュータ読み取り可能な記録媒体。

図1



デジタルデータ記録装置

図2

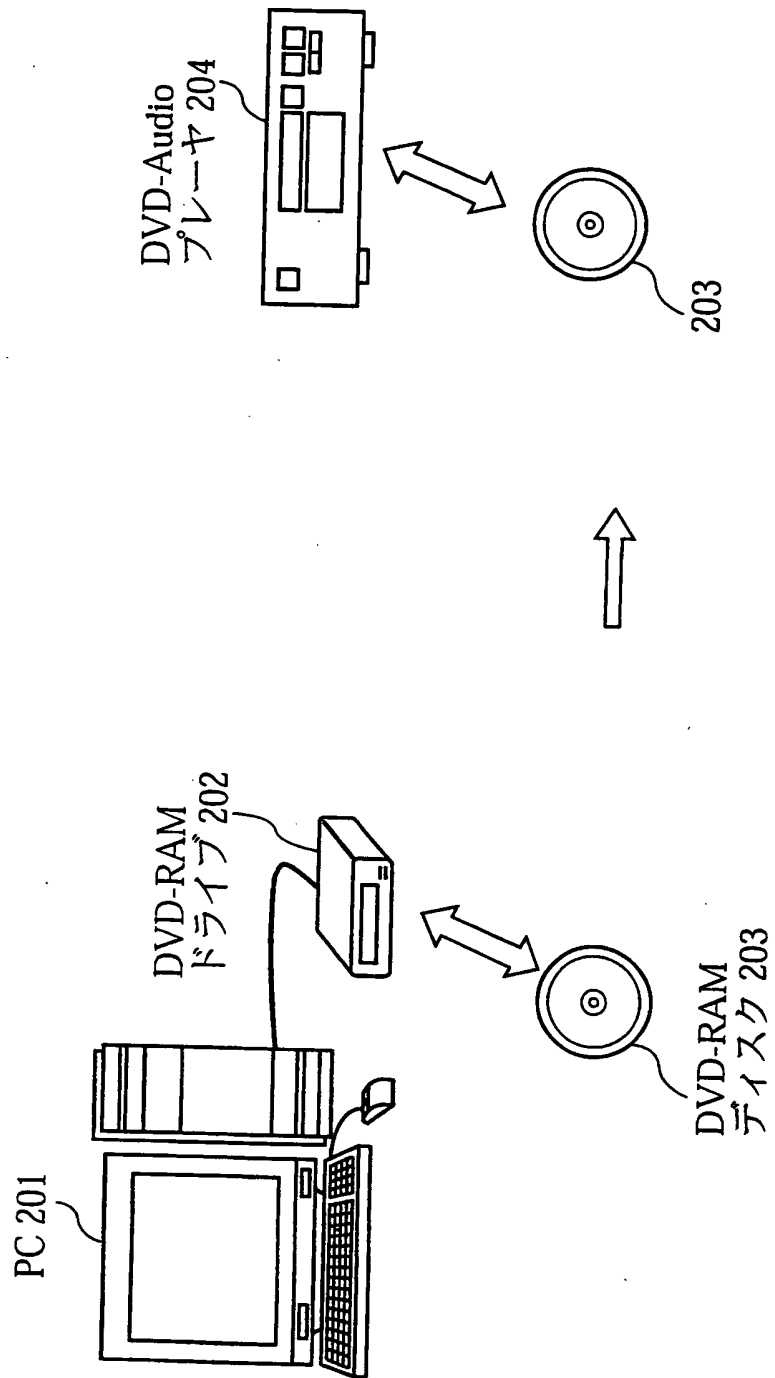


図3

301 曲名	302 歌手名	303 収録時間	304 価格
Song1	SingerA	4分20秒	100円
Song2	SingerB	3分53秒	50円
Song3	SingerC	4分48秒	75円
Song4	SingerD	4分06秒	100円
:	:	:	:
:	:	:	:

図4

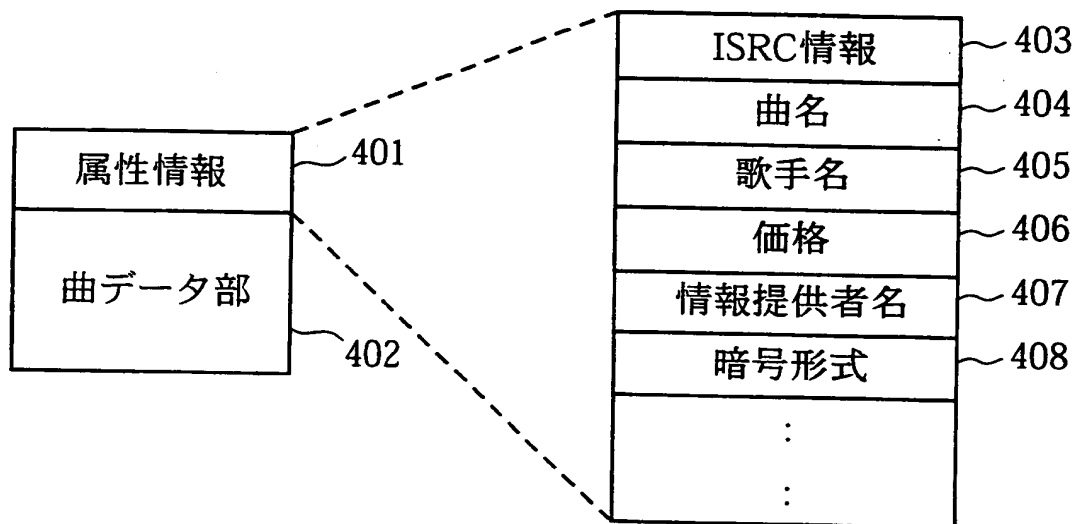


図5

301 曲名	302 歌手名	303 収録時間	501 価格(1)	502 価格(2)
Song1	SingerA	4分20秒	100円	70円
Song2	SingerB	3分53秒	50円	35円
Song3	SingerC	4分48秒	75円	50円
Song4	SingerD	4分06秒	100円	100円
:	:	:	:	:
:	:	:	:	:

図6

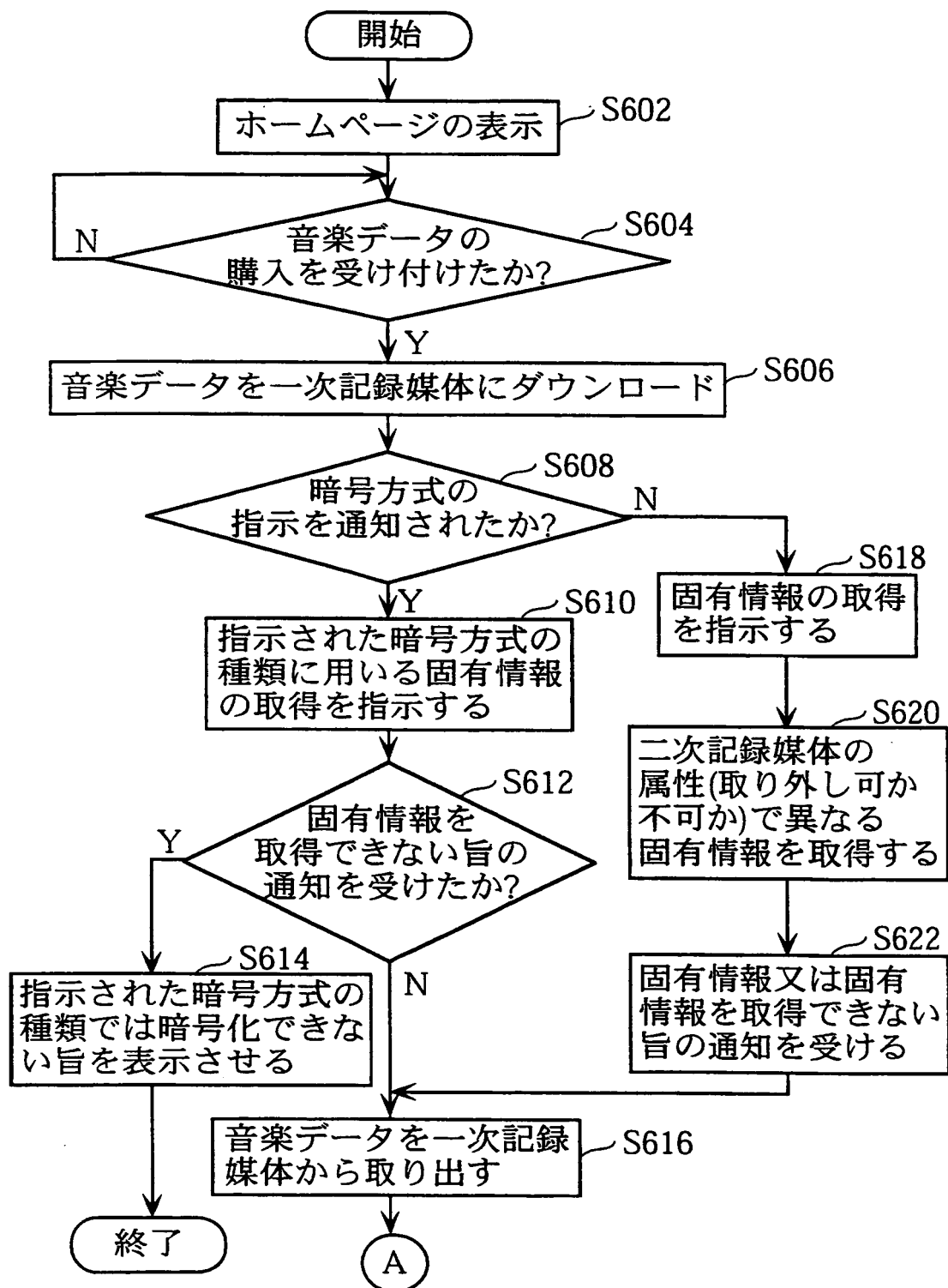


図7

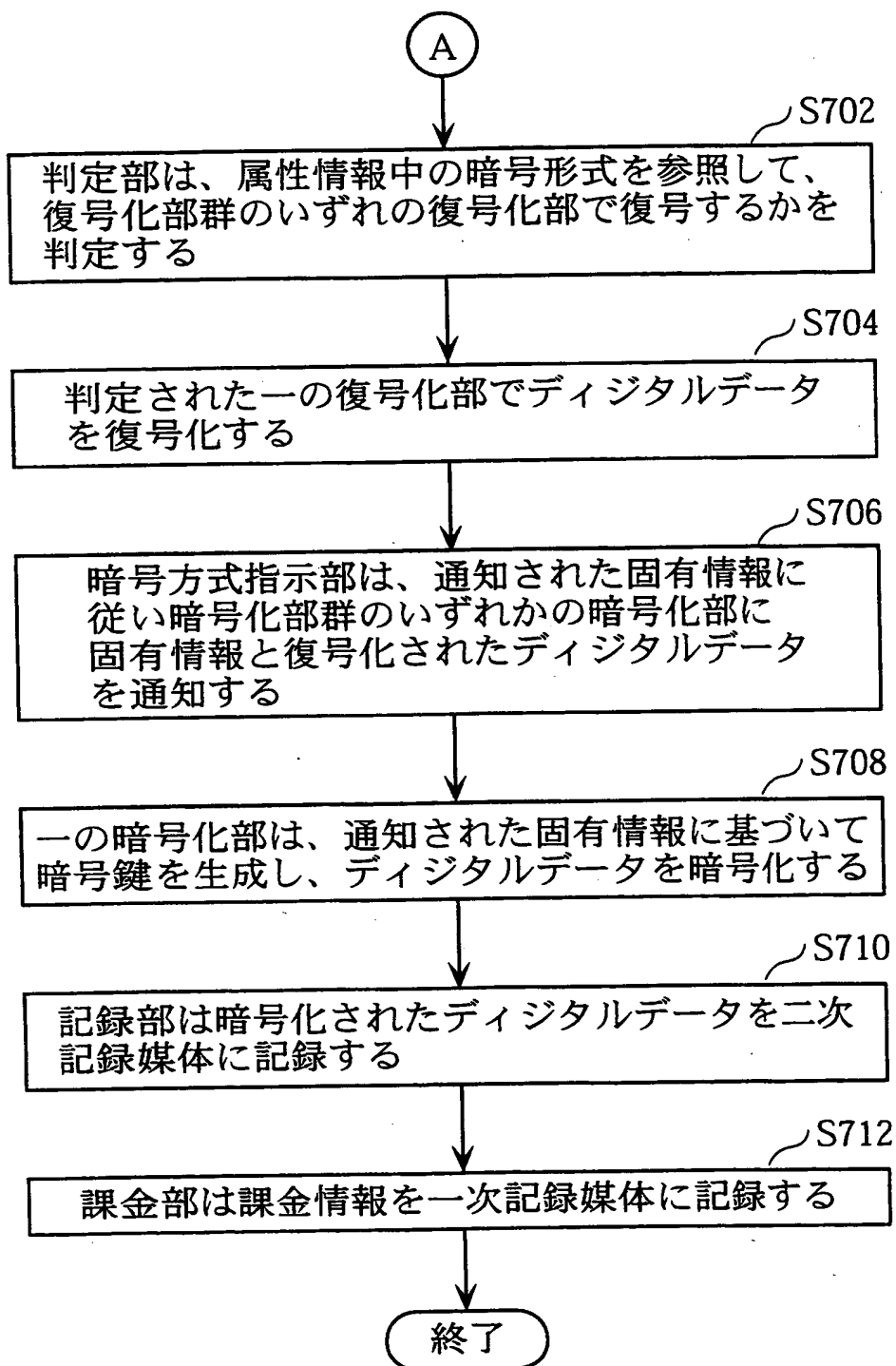


図8

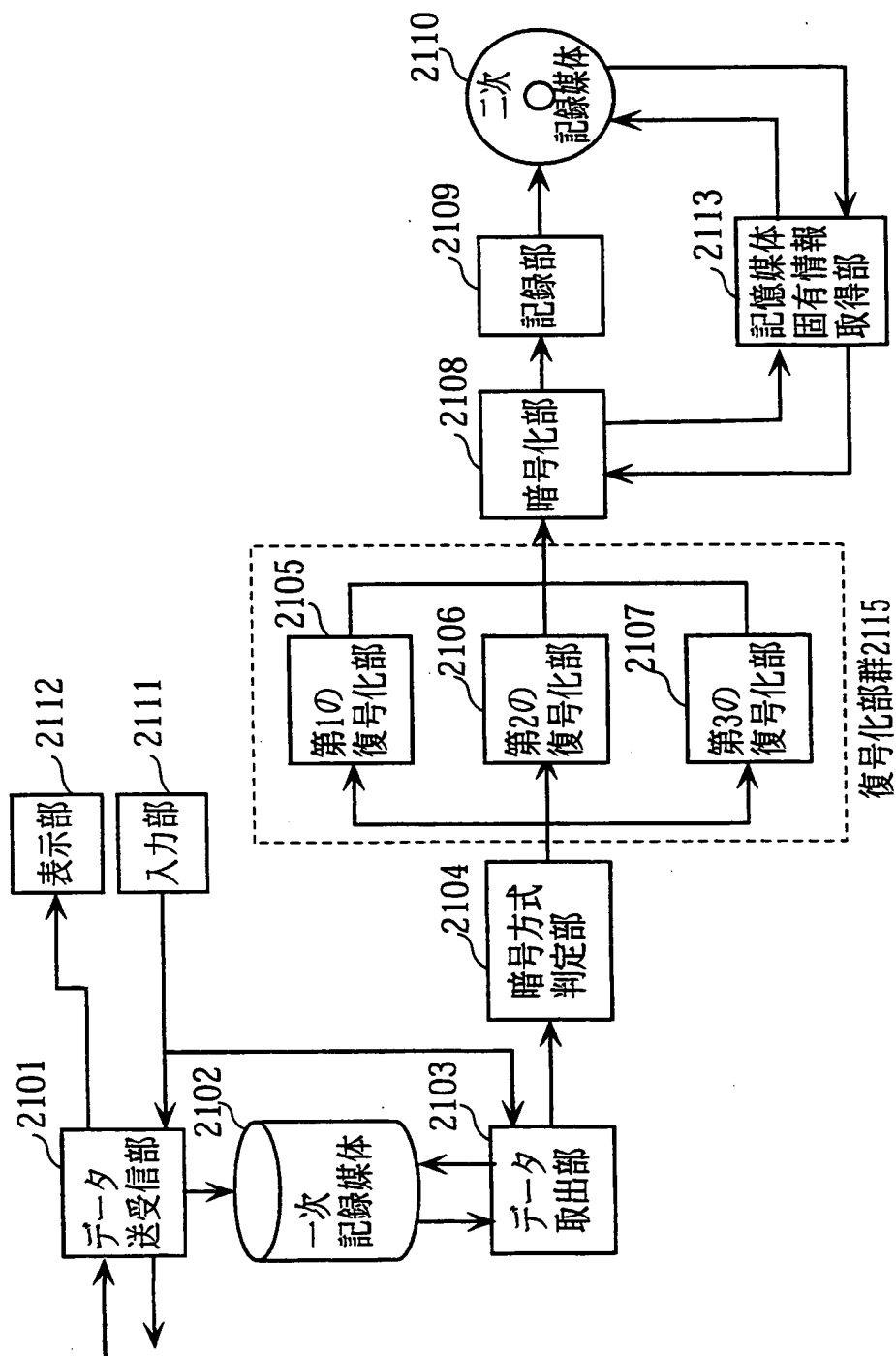


図9

曲名	曲名コード	歌手名	データ入手先
曲A	song01	A	www. song/song01
曲B	song02	B	www. song/song02
曲C	song03	C	www. song/song03
曲D	song04	D	www. song/song04
曲E	song05	E	www. song/song05

図10

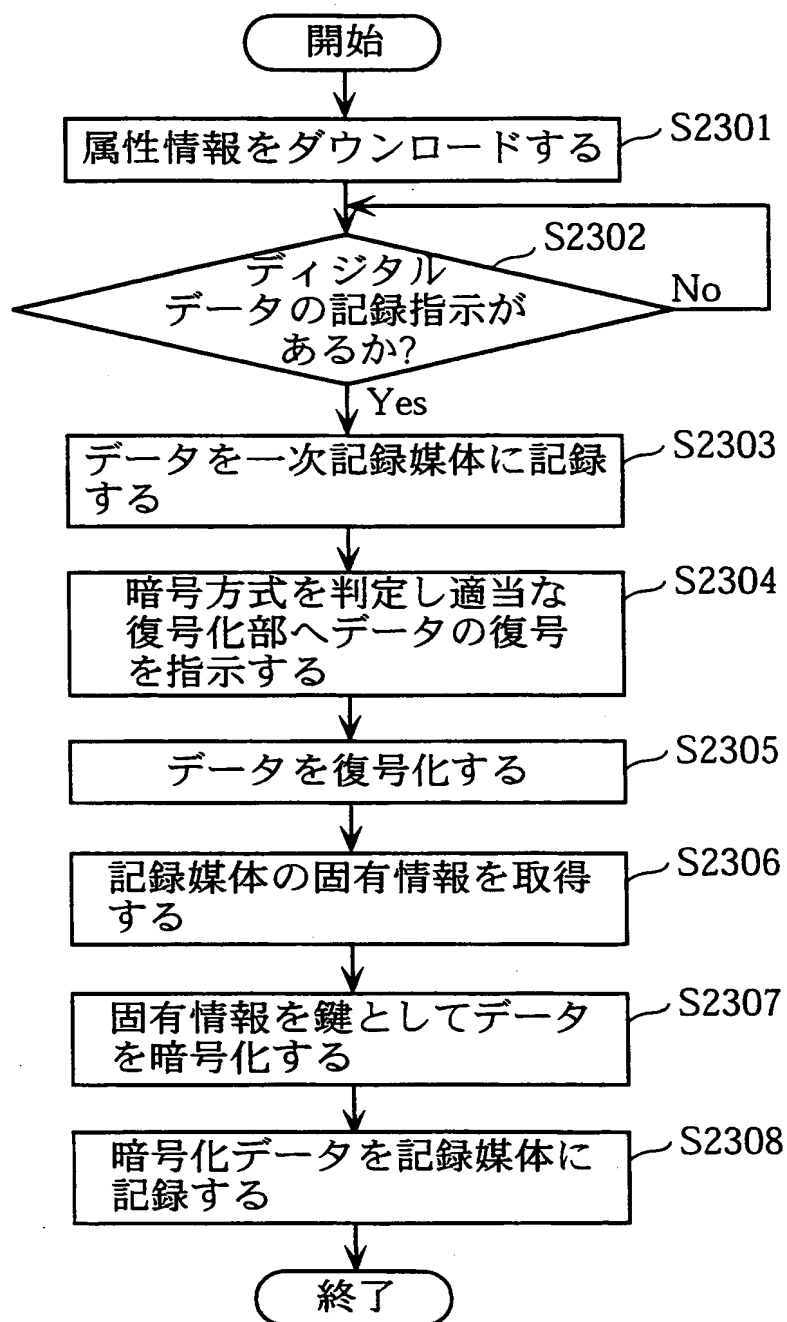


図11

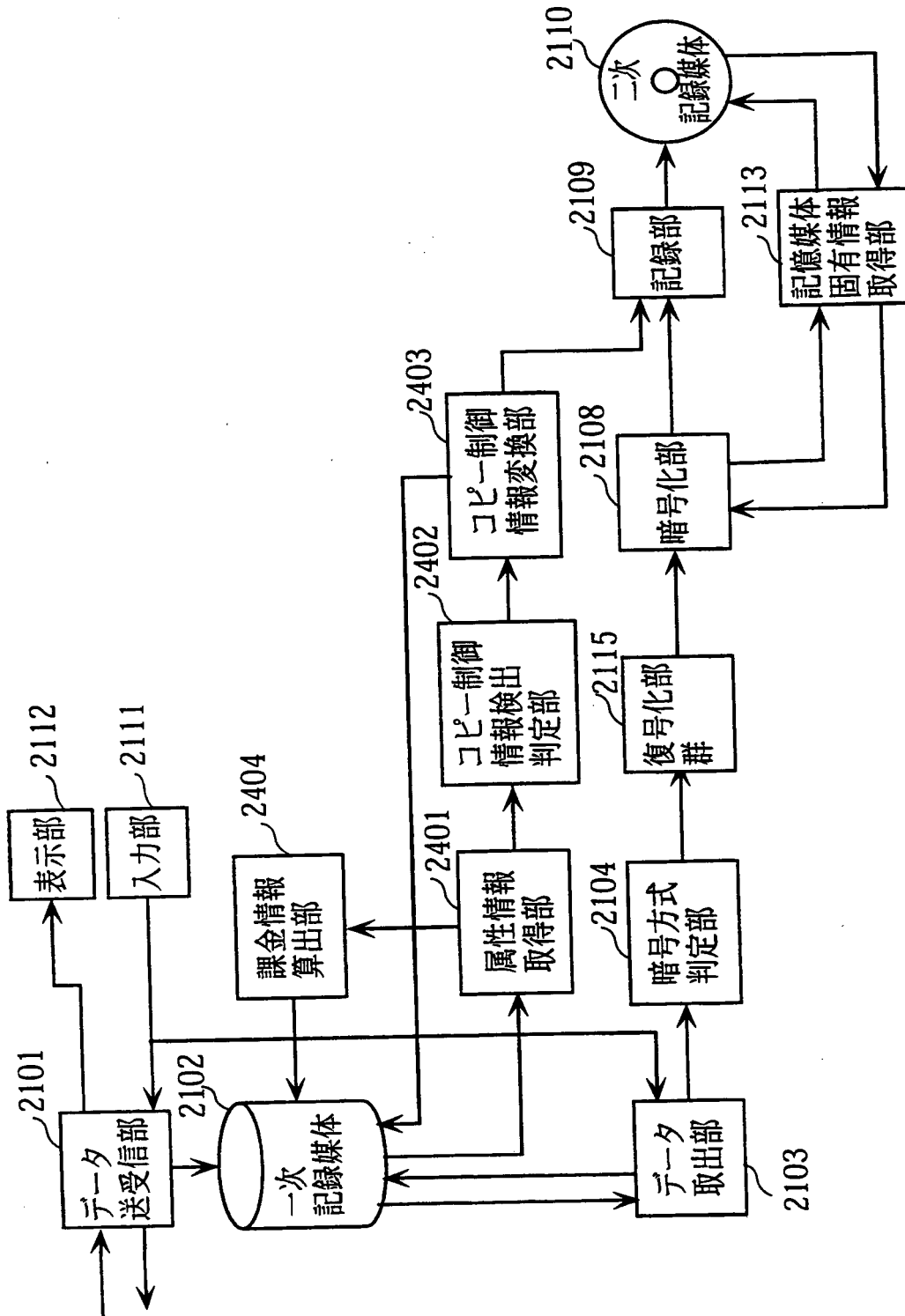


図12

2201		2202		2203		2204		2501		2502	
曲名	曲名コード	歌手名	データ入手先			コピー制御情報			価格		
曲A	song01	A	www. song/song01			孫コピー不可			100円		
曲B	song02	B	www. song/song02			無制限に許可			10円		
曲C	song03	C	www. song/song03			孫コピー不可			0円		
曲D	song04	D	www. song/song04			孫コピー不可			30円		
曲E	song05	E	www. song/song05			2回コピー可			10円		

図13

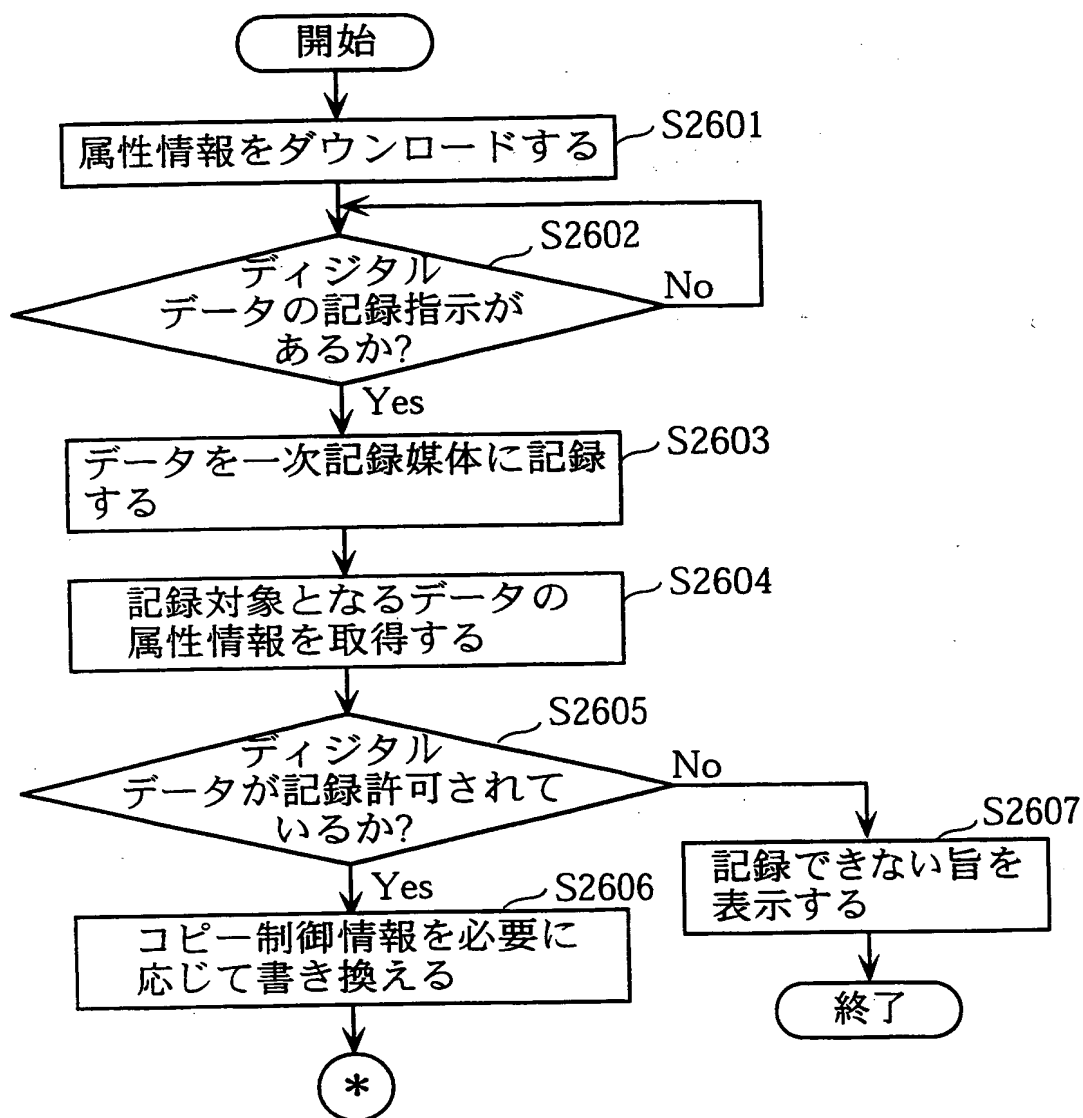


図14

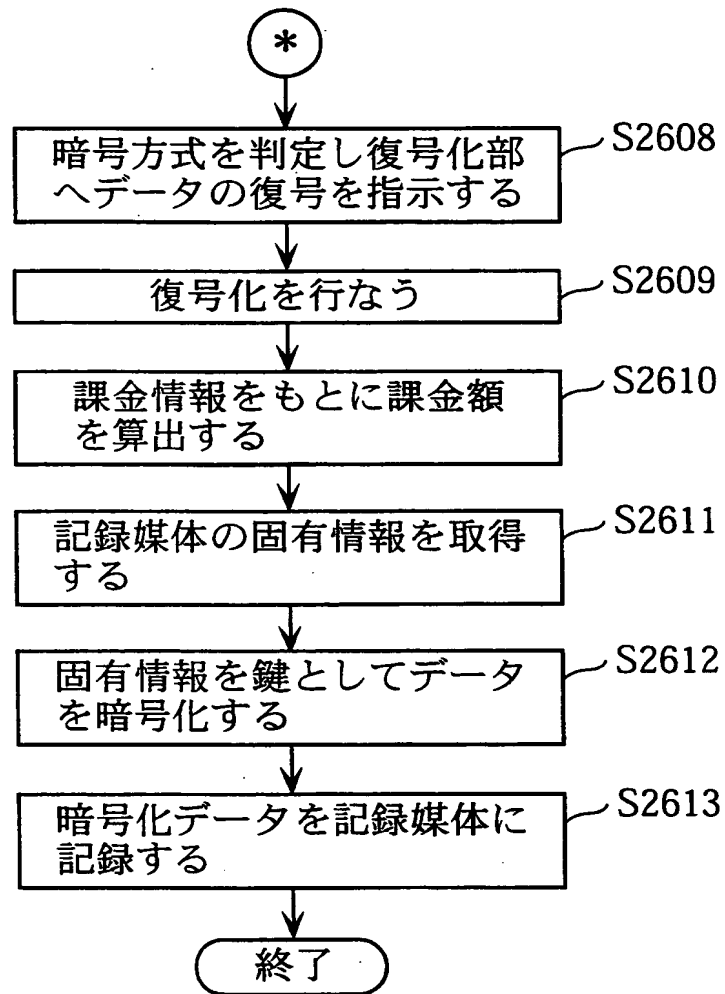


図15

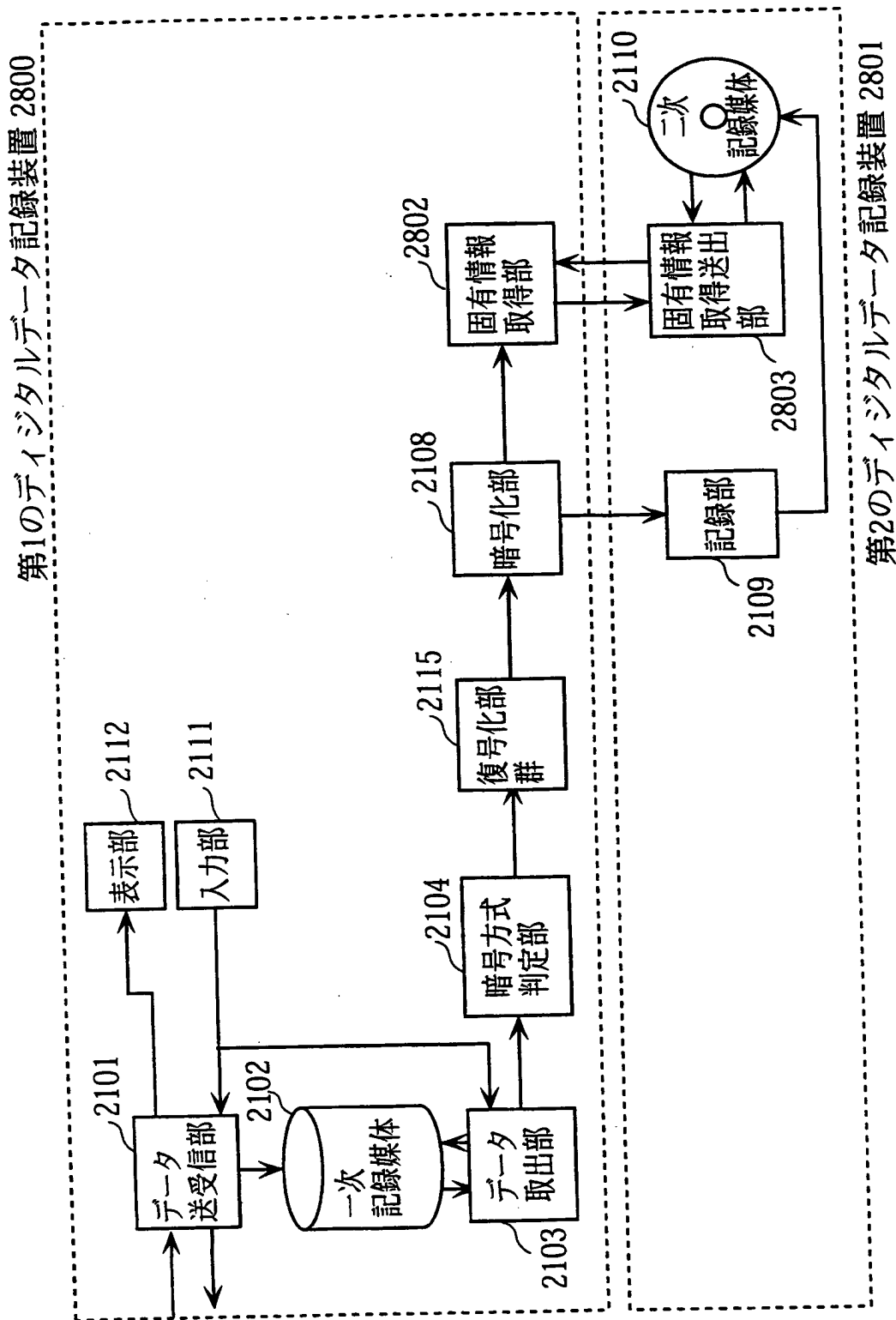


図16

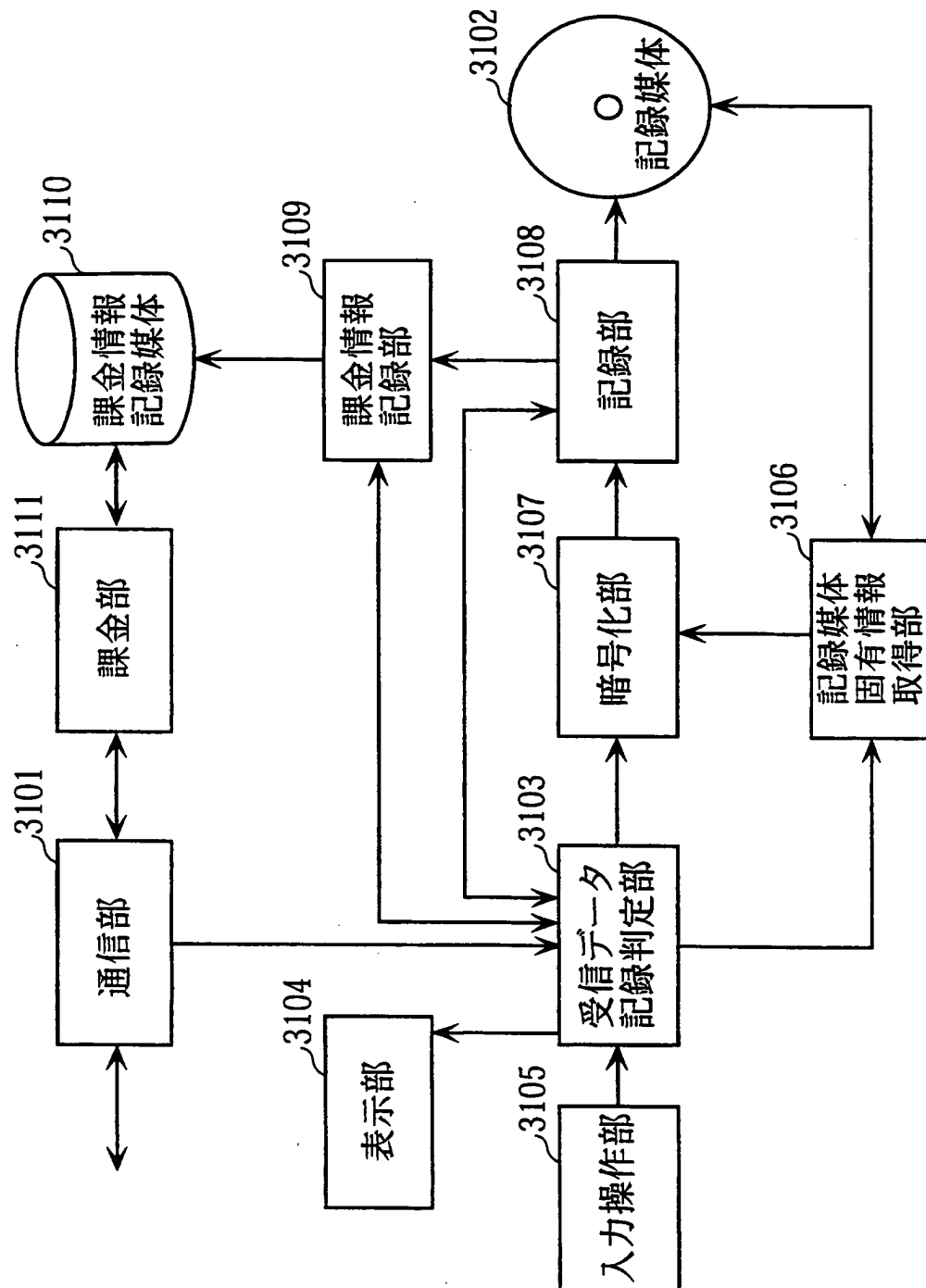


図17

属性情報 3201

曲名	演奏者	曲名コード	記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可	...
曲A	a	song01	100円	0.5円	100回	暗号あり	1回のみ可	...
曲B	b	song02	10円	0円	無限	暗号なし	許可	...
曲C	c	song03	0円	1円	50回	暗号あり	1回のみ可	...
曲D	d	song04	30円	5円	50回	暗号あり	1回のみ可	...
曲E	e	song05	10円	0円	10回	暗号なし	許可	...

図18

管理情報 3301		
3204	3302	3303
曲名コード	記録開始 アドレス	記録終了 アドレス
song01	00320	00933
song02	14902	15172
song03	13085	13994
song04	50870	51825
song05	58349	58783

図19

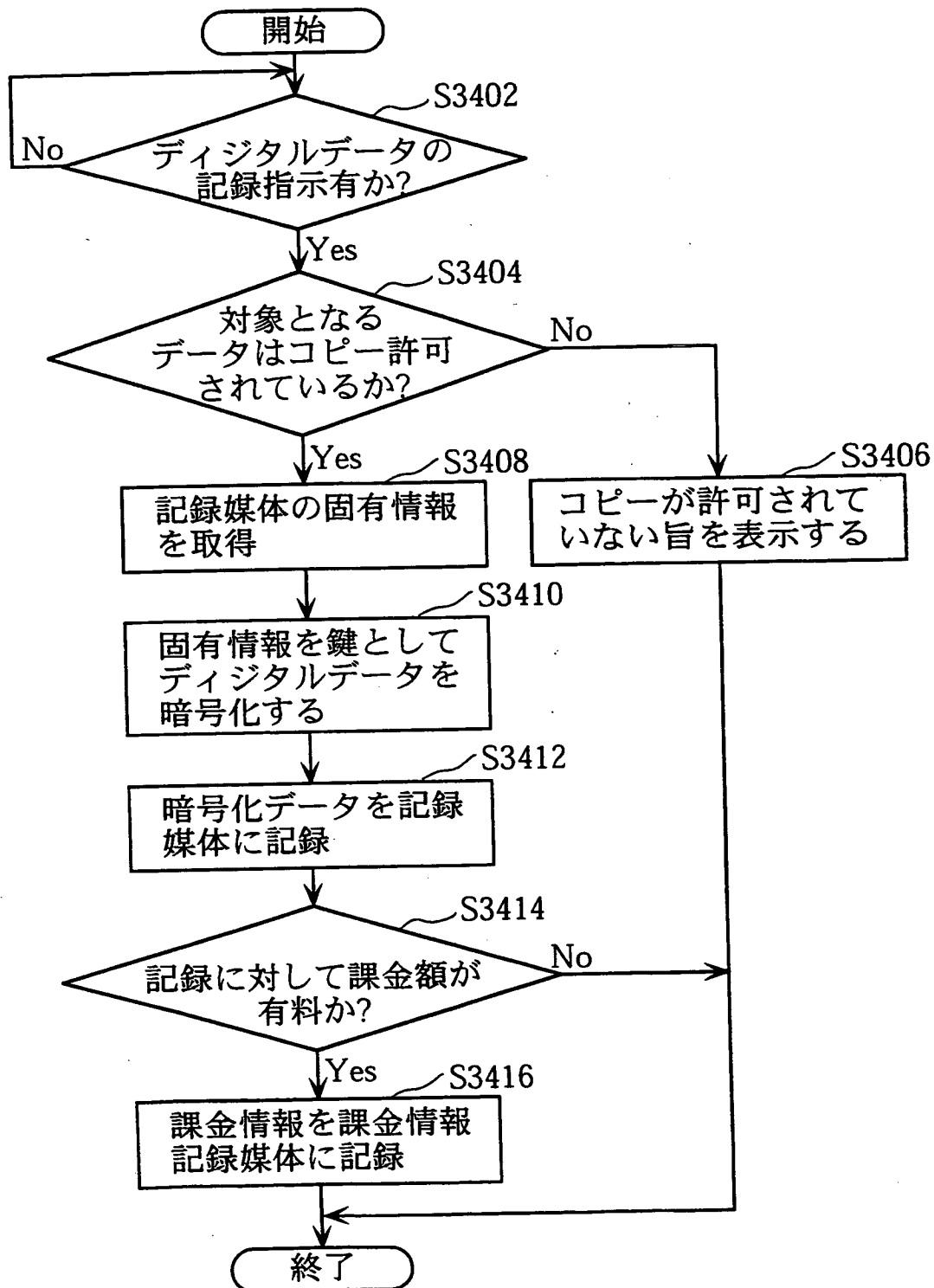


図20

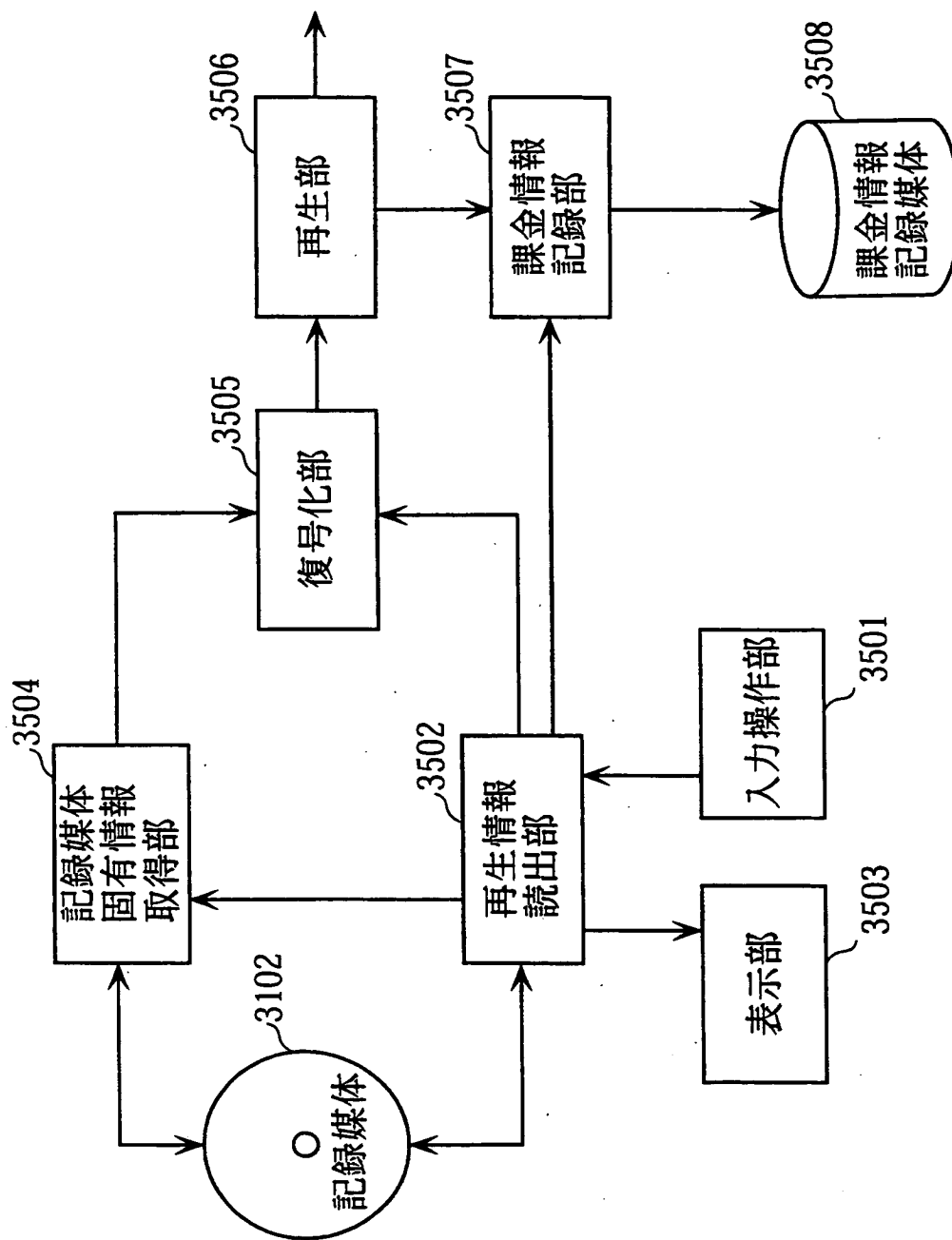


図21

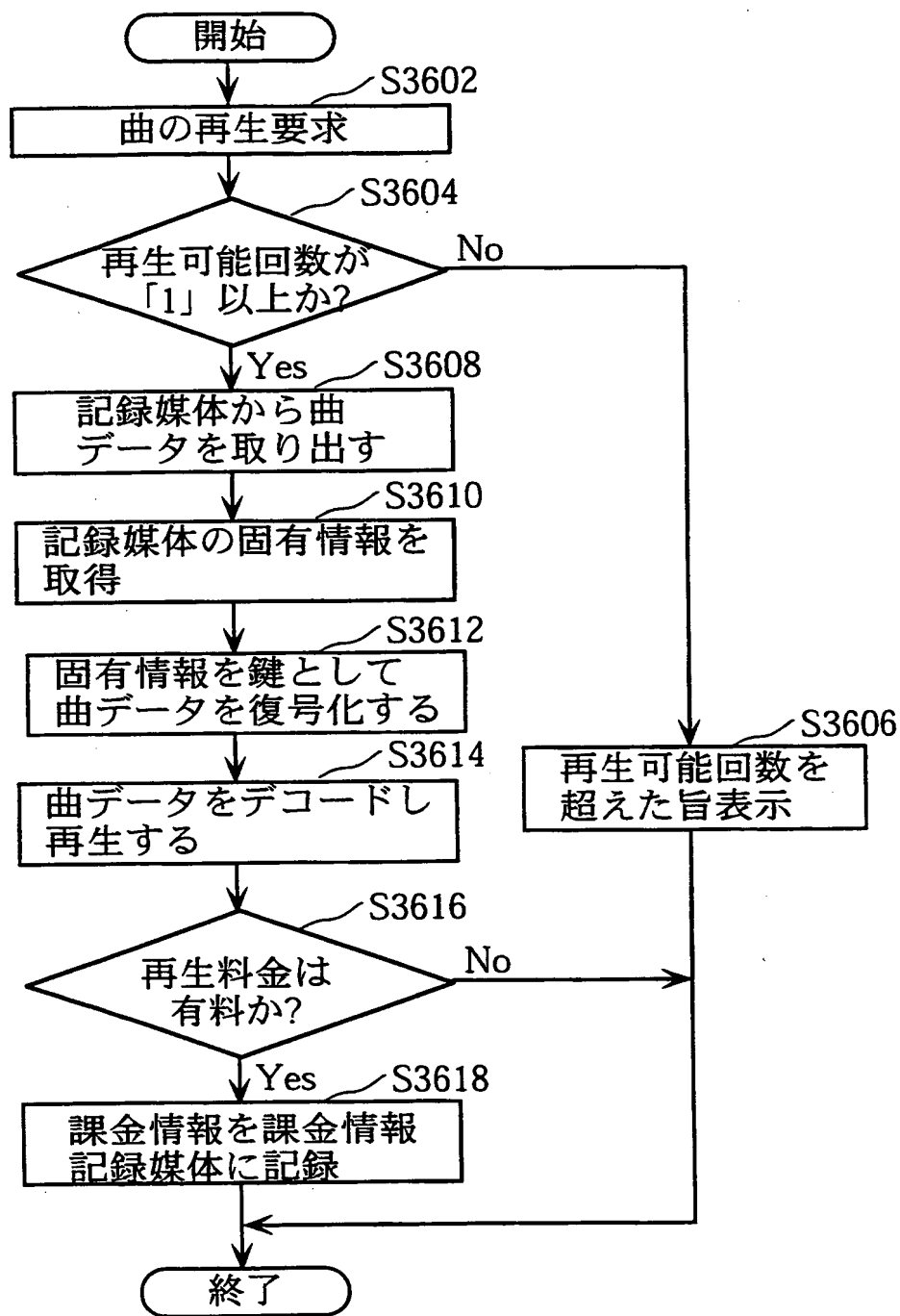


図23

属性情報 3801											
3805			3802			3803					3804
曲名	演奏者	曲名コード	1次記録料金	2次記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可(1次)	コピー許可(2次)	...	
曲A	a	song01	0円	100円	0.5円	100回	暗号あり	1回のみ可	1回のみ可	...	
曲B	b	song02	10円	10円	0円	無限	暗号なし	許可	許可	...	
曲C	c	song03	0円	0円	1円	50回	暗号あり	1回のみ可	1回のみ可	...	
曲D	d	song04	0円	30円	5円	50回	暗号あり	1回のみ可	1回のみ可	...	
曲E	e	song05	—	—	—	—	暗号なし	不許可	不許可	...	

図24

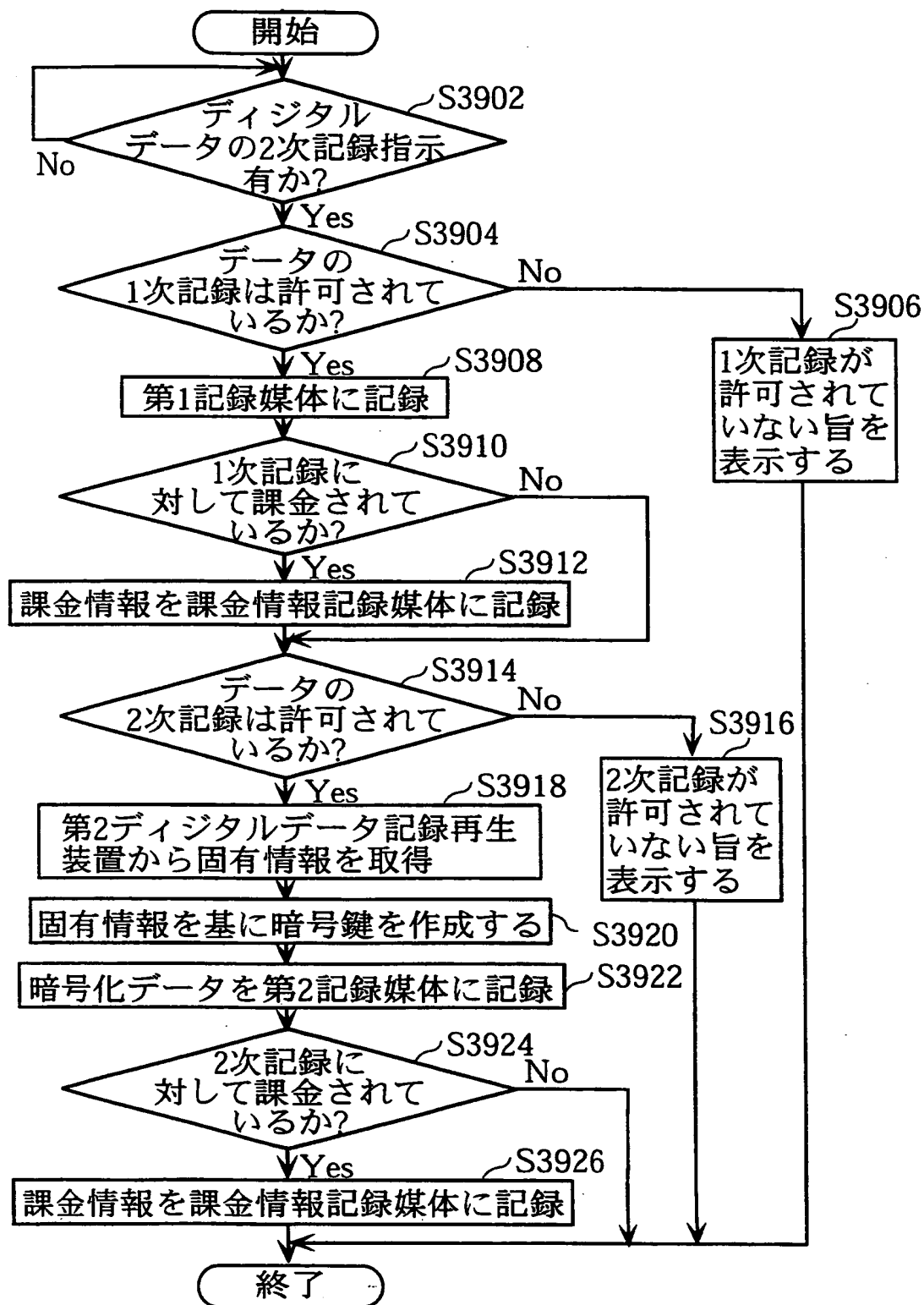


図25

		属性情報31001		31003 31002 31004		31005		2次記録料金	
...	...	曲名コード	...	媒体ID	機器ID	媒体ID+機器ID
...	...	song01	...	100円	10円	10円	...	10円
...	...	song02	...	10円	1円	1円	...	1円
...	...	song03	...	0円	0円	0円	...	0円
...	...	song04	...	30円	3円	3円	...	3円
...	...	song05	...	10円	1円	1円	...	1円

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/03887

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁶ G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁶ G11B20/10Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1999 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 7-272399, A (Hitachi, Ltd.), 20 October, 1995 (20. 10. 95), Full text ; Figs. 1 to 18 & US, 5912969, A	1-12
A	JP, 8-339629, A (Matsushita Electric Industrial Co., Ltd.), 24 December, 1996 (24. 12. 96), Full text ; Figs. 1 to 4 (Family: none)	1-12
P, A	JP, 11-191266, A (Kobe Steel, Ltd.), 13 July, 1999 (13. 07. 99), Full text ; Figs. 1, 2 (Family: none)	1-12

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

- * Special categories of cited documents:
- "A" document defining the general state of the art which is not considered to be of particular relevance
 - "E" earlier document but published on or after the international filing date
 - "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 - "O" document referring to an oral disclosure, use, exhibition or other means
 - "P" document published prior to the international filing date but later than the priority date claimed
 - "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 - "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 - "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 - "&" document member of the same patent family

Date of the actual completion of the international search
19 October, 1999 (19. 10. 99)Date of mailing of the international search report
2 November, 1999 (02. 11. 99)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl⁶ G11B20/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl⁶ G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1999年
日本国公開実用新案公報	1971-1999年
日本国登録実用新案公報	1994-1999年
日本国実用新案登録公報	1996-1999年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 7-272399, A (株式会社日立製作所) 20. 10月. 1995 (20. 10. 95) 全文, 第1-18図 & US, 5912969, A	1-12
A	J P, 8-339629, A (松下電器産業株式会社) 24. 12月. 1996 (24. 12. 96) 全文, 第1-4図 (ファミリーなし)	1-12
P, A	J P, 11-191266, A (株式会社神戸製鋼所) 13. 7月. 1999 (13. 07. 99) 全文, 第1-2図 (ファミリーなし)	1-12

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日
19. 10. 99

国際調査報告の発送日
02.11.99

国際調査機関の名称及びあて先
日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
小松 正



5 Q 7736

電話番号 03-3581-1101 内線 6922

THIS PAGE BLANK (USPTO)